Kristina Peters (Hg.)

CYBERKRIMINALITÄT

AKTUELLE HERAUSFORDERUNGEN FÜR POLIZEI, STAATSANWALTSCHAFT, GERICHTE UND WISSENSCHAFT

Dieser Sammelband ist das Ergebnis einer Vortragsreihe, die im Wintersemester 2021/2022 an der Ludwig-Maximilians-Universität München unter der Verantwortung von Dr. Kristina Peters stattgefunden hat. Die Aufzeichnungen der Originalvorträge sind verfügbar auf:

[1]

DOI: 10.5282/ubm/epub.92172
https://doi.org/10.5282/ubm/epub.92172

München 2022

[1] https://icons8.com/icon/108794/youtube-quadratisch

INHALT

VORWORT

Es wird aktuell heftig diskutiert, inwieweit das derzeitige Strafrecht den Herausforderungen der Digitalisierung gerecht wird. Gleichzeitig haben gerade in der jüngeren Vergangenheit vielfältige gesetzgeberische Aktivitäten zu einer hohen Dynamik in dem sonst eher trägen Bereich strafrechtlicher Normen geführt.

Eine wissenschaftliche Auseinandersetzung mit der Strafbarkeit von neuen Erscheinungsformen von Kriminalität sollte jedoch auch die Erfahrungen der Strafverfolgungsorgane sowie entsprechender Interessenvereinigungen in die Überlegungen einbeziehen. Auch ist zu erwarten, dass viele der Studierenden, die momentan ausgebildet werden und sich für einen Beruf mit strafrechtlichem Einschlag entscheiden – sei es bei der Staatsanwaltschaft, einem Gericht, einem Ministerium, in der Strafverteidigung oder einer NGO – in ihrem Berufsleben mit den Konsequenzen konfrontiert werden, welche die voranschreitende Digitalisierung im Bereich des Strafrechts hat. In der juristischen Ausbildung kommen diese Themen jedoch bislang kaum vor, was auch mit der Ausrichtung auf das Staatsexamen mit seinem umfangreichen Programm, das gleichzeitig Themen der Digitalisierung bislang weitgehend ausspart, zusammenhängt. Hier ist sowohl ein enormes Bedürfnis nach entsprechend qualifiziertem Nachwuchs auf der Seite der Praxis als auch ein reges Interesse vieler Studierender an diesen Themen zu identifizieren.

In diese Lücke stieß die Vortragsreihe „Cyberkriminalität – Aktuelle Herausforderungen für Polizei, Staatsanwaltschaften, Gerichte und Wissenschaft“, die im Wintersemester 2021/22 an der Ludwig-Maximilians-Universität München stattfand. Ihre Ergebnisse fasst der vorliegende Sammelband zusammen.

Zum Auftakt der Vortragsreihe war **Linus Neumann** zu Gast, ein führender deutscher Netzpolitiker und Sprecher der Nichtregierungsorganisation Chaos Computer Club, der regelmäßig als Sachverständiger im Bundestag zu Themen der IT-Sicherheit tätig ist. Sein Vortrag trug den Titel „Cybercrime – Zwischen Kriminalisierung und Eigenverantwortung“ und erläuterte detailliert den Ablauf eines Hackerangriffs. Gleichzeitig wurden Möglichkeiten aufgezeigt, welche Schutzmaßnahmen von privater sowie staatlicher Seite unternommen werden können, und die Frage diskutiert, wie effektiv eine strafrechtliche Reaktion ist und sein könnte. Eine schriftliche Fassung dieses spannenden Vortrags liegt leider nicht vor – er steht aber weiterhin auf Youtube zur Verfügung und sei interessierten Leserinnen und Lesern mit Nachdruck ans Herz gelegt.

Der zweite Vortrag stammte von der Veranstalterin der Vortragsreihe und Herausgeberin dieses Sammelbandes. Dr. **Kristina Peters** ist am Lehrstuhl für Strafrecht, Strafprozessrecht, Rechtsphilosophie und Rechtssoziologie der Juristischen Fakultät der Ludwig-Maximilians-Universität München tätig. Sie befasste sich unter der Überschrift „Cyberkriminalität im aktuellen Strafrecht“ mit der Frage, welche Erscheinungsformen von Cybercrime nach derzeitigem Stand strafbar sind. Wo verlaufen die Grenzen der Strafbarkeit – und besteht hier Handlungsbedarf?

Im Anschluss war das Bundeskriminalamt zu Gast: **Florian Kreikemeyer** von der Abteilung Cybercrime berichtete unter der Überschrift „Modi Operandi im Netz“ von der Ermittlungsarbeit der Polizei. Von Phishing, DDoS- über Ransomware-Angriffe wurden die häufigsten Erscheinungsformen von Straftaten gegen informationstechnische Systeme vorgestellt. Es wurde eindrücklich beschrieben, dass sich mittlerweile ein globaler Markt für Cybercrime-as-a-service entwickelt hat, auf dem auch technisch weniger versierte Personen gezielt kriminelle Dienstleistungen für die Begehung von Straftaten erwerben können. Aufgrund der sensiblen Inhalte, die das Bundeskriminalamt anlässlich dieses Vortrags mit den Zuhörerinnen und Zuhörern teilte, liegt leider weder eine Aufzeichnung noch eine schriftliche Fassung des Beitrags vor. Interessierte Leserinnen und Leser können sich aber hier einen näheren Überblick über die Arbeit der Abteilung Cybercrime verschaffen.

Für einen umfassenden Blick auf die Arbeit der Strafverfolgungsorgane ergänzte **Thomas Goger**, Oberstaatsanwalt im Zentrum zur Bekämpfung von Kinderpornographie und sexuellem Missbrauch im Internet bei der Zentralstelle Cybercrime Bayern, die Ausführungen des Bundeskriminalamts. Im Fokus stand das Vorgehen der Zentralstelle gegen den signifikanten Anstieg registrierter einschlägiger Straftaten. Besonders kontrovers wurde die Möglichkeit einer Verkehrsdatenspeicherung diskutiert, da die aktuelle Rechtslage es den Ermittlerinnen und Ermittlern vielfach unmöglich mache, die Taten einzelnen Täterinnen und Tätern zuzuordnen.

Einen Blick auf die Perspektive der Opfer eröffnete im Anschluss **Josephine Ballon**, Head of Legal bei der gemeinnützigen Organisation HateAid, mit ihrem Vortrag über „Digitale Gewalt – Möglichkeiten und Herausforderungen bei ihrer Bekämpfung“. HateAid bietet Beratungen und Prozesskostenhilfe für Betroffene von digitalen Beleidigungen und Hassnachrichten an und vertrat in der Vergangenheit etwa Renate Künast und die Klimaaktivistin Luisa Neubauer. Ausgehend von einem großen Erfahrungsschatz wurde eindrücklich beschrieben, welche Hürden bei der Verfolgung digitaler Beleidigungen und Bedrohungen bestehen.

Zum Abschluss der Reihe wurde schließlich die Perspektive gewechselt und danach gefragt, inwieweit die voranschreitende Digitalisierung nicht nur eine Bedrohung darstellt, sondern umgekehrt bei der Verfolgung von Straftaten behilflich sein kann. „Künstliche Intelligenz" ist eines der großen Buzzwords unserer Zeit. Doch was kann sie wirklich leisten – und wo sind die Erwartungen, die mit ihr verbunden werden, zu hoch? Diese Frage stellt sich auch und besonders mit Blick auf einen Einsatz Künstlicher Intelligenz in der Strafverfolgung. Dr. **Ludwig Bothman** vom Lehrstuhl für Statistical Learning and Data Science am Institut für Statistik der Ludwig-Maximilians-Universität München gab zum Abschluss der Vortragsreihe einen spannenden Überblick über die Möglichkeiten und Grenzen eines Einsatzes von KI.

Sämtliche Vorträge, die aufgezeichnet werden durften, sind weiterhin hier zu finden.

Die Veranstalterin der Vortragsreihe dankt allen Referentinnen und Referenten für die interessanten und gewinnbringenden Vorträge sowie den Zuhörerinnen und Zuhörern für die regen Diskussionen. Besonderer Dank für Hilfe und Unterstützung bei der Durchführung der Vortragsreihe und der Erstellung dieses Sammelbandes ist Herrn stud. iur. Jonathan-Milot Spörl geschuldet.

Die Durchführung der Vortragsreihe und die Veröffentlichung dieses Sammelbandes wurde durch LMUexcellent im Rahmen der Exzellenzstrategie von Bund und Ländern ermöglicht.

München, September 2022 *Kristina Peters*

CYBERKRIMINALITÄT IM AKTUELLEN STRAFRECHT

KRISTINA PETERS

Dr. Kristina Peters, Wissenschaftliche Mitarbeiterin und Habilitandin am Lehrstuhl für Strafrecht, Strafprozessrecht, Rechtsphilosophie und Rechtssoziologie von Professor Dr. Armin Engländer, Ludwig-Maximilians-Universität München.

Der folgende Beitrag gibt einen Überblick über das materielle Strafrecht. Im Kern steht die Frage, was das geltende Strafrecht der Cyberkriminalität entgegenzusetzen hat. Dabei wird nach einer kurzen Einleitung (I.) zunächst erörtert, ob es sich bei Cyberkriminalität um ein Modethema oder um eine ernste Bedrohung handelt (II). Sodann wird herausgearbeitet, welche Handlungen derzeit strafbar sind (III.) und schließlich vor diesem Hintergrund der Frage nachgegangen, ob insoweit ein gesetzgeberischer Handlungsbedarf besteht (IV.).

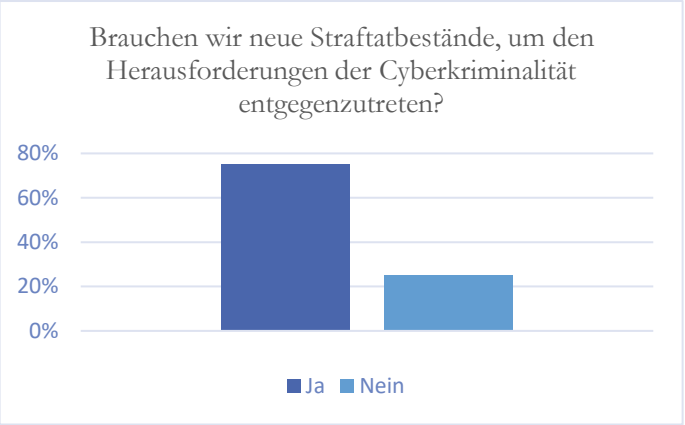
I. Cyberkriminalität

Befasst man sich mit Cyberkriminalität, so stößt man auf ganz unterschiedliche Themen, mit denen man sich befassen kann. Da sind zum einen die *Modi operandi* – die Art, wie sich Taten im Bereich der Cyberkriminalität phänotypisch für Ermittlerinnen und Ermittler darstellen.[1] Zudem drängt sich die Frage auf, wie Privatpersonen sich effektiv gegen Akte der Cyberkriminalität schützen können und wieviel Eigenverantwortung und Selbstschutz hier gefordert wird.[2] Und schließlich stellt sich das Problem, wie eine effektive Strafverfolgung von Cyberkriminalität gelingen kann und welche besonderen Herausforderungen sich hier ergeben.[3]

All diese Fragen stehen an anderen Stellen dieses Sammelbandes mehr oder weniger im Fokus, bilden jedoch nicht das Thema des vorliegenden Beitrags. Dieser widmet sich stattdessen dem materiellen Strafrecht – also der Frage danach, was aktuell überhaupt strafbar ist. Anders formuliert: Was steht eigentlich zum Thema Cyberkriminalität im Strafgesetzbuch (StGB)? Dabei wird es auch um die Frage gehen, ob das Strafrecht in seiner aktuellen Kodifizierung die rasanten Entwicklungen noch abdecken kann oder ob es neue Straftatbestände braucht.

> Braucht es neue Straftatbestände, um die rasanten Entwicklungen abzudecken?

1 Siehe hierzu den interessanten Überblick des Bundeskriminalamts.
2 Siehe hierzu den Vortrag von Linus Neumann.
3 Siehe hierzu insbesondere den Vortrag von Josephine Ballon sowie den entsprechenden Beitrag in diesem Band.



Grafik: Umfrageergebnis aus der Vortragsreihe

II. Cybercrime: „Modethema“ oder ernste Bedrohung?

1. Statistisches Material

Wenden wir uns der ersten Frage zu: Ist Cybercrime eigentlich ein Modethema oder eine ernste Bedrohung? Das Thema „Kriminalität“ beschäftigt gesellschaftliche wie private Diskussionen, wird medial teils exzessiv aufbereitet und verwertet und gerne genutzt, um politische Handlungen zu rechtfertigen. Die konkreten Daten zur Ermittlungsarbeit der Polizei[4] und zu den Verurteilungen durch Gerichte[5] sind öffentlich einsehbar, sind hinter keiner Paywall verborgen oder nur für Angehörige von Behörden zugänglich. Trotzdem wird häufig völlig losgelöst von den konkreten Zahlen berichtet und diskutiert.

> Das Thema „Kriminalität“ wird medial teils exzessiv aufbereitet

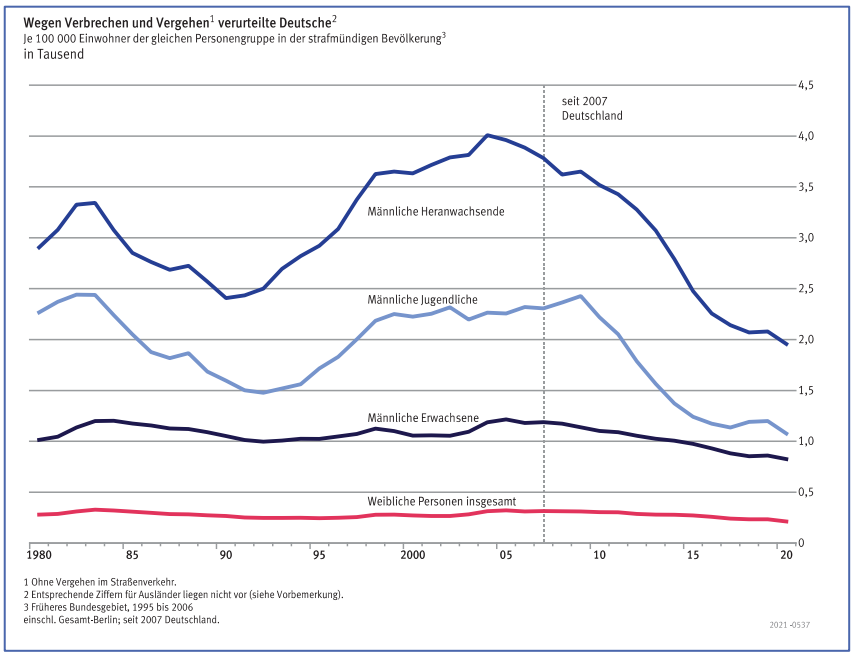
a) Das allgemeine Kriminalitätsniveau in Deutschland

Zunächst lohnt ein Blick auf das allgemeine Kriminalitätsniveau in Deutschland. Auch wenn man es bei einem Blick auf die mediale Berichterstattung kaum glauben mag: Hier lautet die wichtigste Erkenntnis, dass die Anzahl der registrierten Straftaten seit Jahrzehnten abnimmt.[6]

4 Interessant ist hier insbesondere die Polizeiliche Kriminalstatistik (PKS).

5 Die Verurteilungszahlen werden durch das Statistische Bundesamt veröffentlicht: Fachserie 10 (Rechtspflege), Reihe 3 (Strafverfolgung).

6 Zur Vertiefung siehe etwa *Neubacher,* Kriminologie, 4. Aufl. 2020, Kapitel 5; *Singelnstein/Kunz*, Kriminologie, Eine Grundlegung, 8. Aufl. 2021, Kapitel 3.



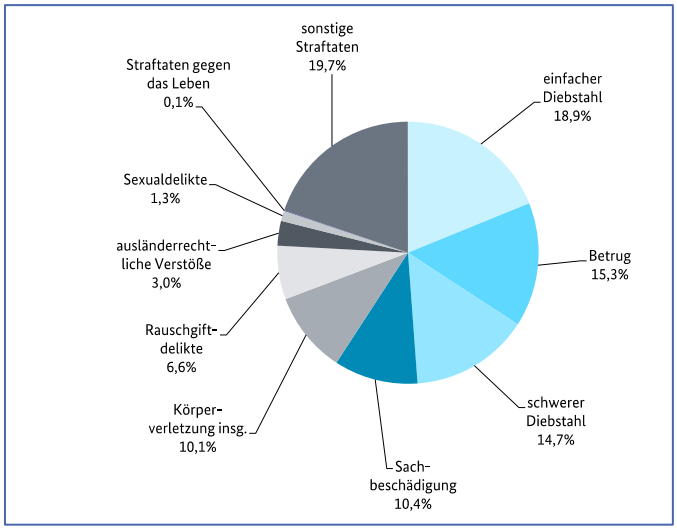
Grafik: Statistisches Bundesamt, Fachserie 10, Reihe 3 (2020), S. 12

> Es darf nicht losgelöst von den konkreten Zahlen berichtet und diskutiert werden

Zwar erkennt man auf der obigen Grafik auf den ersten Blick gewisse Schwankungen. Der Grund dafür, dass die Kurve ab ungefähr 1990 vorübergehend anstieg, liegt jedoch darin, dass damals die neuen Bundesländer sukzessive in die Statistik aufgenommen wurden, sodass die absolute Anzahl der Straftaten zunahm. Erst ab 2007 sind alle Bundesländer in der Statistik vertreten – und seitdem nimmt die Kurve wieder kontinuierlich ab. Der Abwärtstrend, der bereits in den 1980er Jahren begonnen hat, setzt sich fort.

> Im Mittel nimmt die Anzahl der registrierten Straftaten stetig ab

b) Welche Straftaten werden am häufigsten begangen?



Grafik: Bundeskriminalamt, PKS 2019, Bd. 1, S. 17. Eine aktualisierte Version der Grafik wurde 2020 und 2021 nicht zur Verfügung gestellt.

> Die Verteilung der einzelnen Delikte spiegelt dabei nicht immer die eigene Intuition wider

Doch welche Straftaten werden eigentlich am häufigsten begangen? Und welche Rolle spielt hier die Cyberkriminalität? Auch hierzu stellen die Behörden aussagekräftige Zahlen bereit. Die Grafik zeigt, dass gewisse Intuitionen unzutreffend sind: Tötungsdelikte werden in Deutschland nur äußerst selten begangen und auch Körperverletzungen führen mitnichten die Liste der häufigsten Straftaten an. Stattdessen bilden ganz klar die Diebstahlsdelikte mit insgesamt etwa 34% die Gruppe der am häufigsten begangenen Delikte. Hierbei handelt es sich um „Alltagskriminalität", die im wahrsten Sinne des Wortes von „Jedermann" (und jeder Frau) begangen wird. Häufig handelt es sich um Bagatelldelikte: So überschreiten unter den polizeilich registrierten Ladendiebstählen rund 40% nicht einmal die Wertgrenze von 15 Euro.[7]

Auf den ersten Blick hat keines der in der Grafik vertretenen Delikte etwas mit Cyberkriminalität zu tun. Gleichzeitig muss man sich natürlich – und das gilt sicherlich bei der Cyberkriminalität nochmal mehr als in anderen Bereichen – vor Augen halten, dass die Statistiken natürlich nur Auskunft über das sogenannte Hellfeld geben.[8] Das Hellfeld betrifft den Teilbereich der Kriminalität, der amtlich registriert und in den Statistiken erfasst wird. Die wichtigsten Informationsquellen stellen insoweit die Polizeiliche Kriminalstatistik (PKS), die Staatsanwaltschaftliche Erledigungsstatistik und die Verurteilungsstatistik dar. Das Hellfeld bildet jedoch nicht die tatsächliche Kriminalität insgesamt ab, sondern nur das Registrierungsverhalten: Erfasst werden nur die Straftaten, die die Behörde entweder selbst wahrnimmt oder die ihr im Wege der Anzeige bekanntwerden. Im Dunkelfeld verbleibt hingegen die Kriminalität, die nicht behördlich erfasst wird. Zuverlässige Aussagen sind entsprechend schwierig. Die empirische Forschung versucht, dieses Dunkelfeld stärker auszuleuchten, etwa durch Dunkelfeldbefragung von Täterinnen und Tätern sowie Opfern. Wirklich solide Erkenntnisse sind jedoch nur schwer zu erlangen. Insoweit ist natürlich gerade mit Blick auf die Cyberkriminalität zu vermuten, dass vieles im Dunkeln bleibt.

> Statistiken können nur Auskunft über das sogenannte Hellfeld geben

> Im Dunkelfeld verbleibt die Kriminalität, die nicht behördlich erfasst wird

c) Und die Cyberkriminalität?

Doch was weiß man nun konkret über die tatsächliche Relevanz von Cyberkriminalität? Wie gesehen nimmt die Kriminalität insgesamt ab und bei der Gruppe der häufigsten Straftaten ist noch nicht wirklich etwas von dem Phänomenbereich der Cyberkriminalität zu sehen. Um

---

7 Bundeskriminalamt, PKS (2021), Tabelle T07, Aufgliederung der Straftaten nach Schadenshöhe.

8 Zur Unterscheidung und Ausleuchtung von Hell- und Dunkelfeld *Neubacher*, Kriminologie, 4. Aufl. 2020, Kapitel 3; *Singelnstein/Kunz*, Kriminologie, Eine Grundlegung, 8. Aufl. 2021, § 15 Rn. 1.

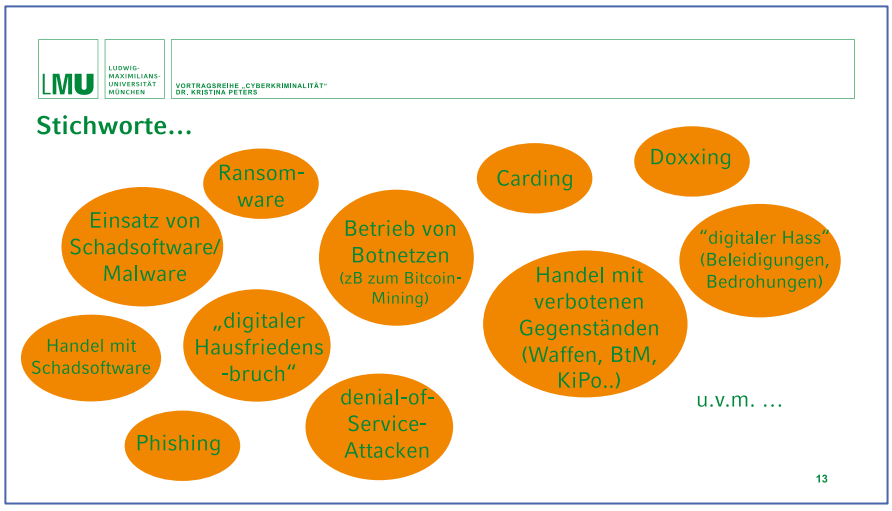
diesen näher auszuleuchten, gilt es, die vorhandenen Statistiken etwas genauer zu studieren. Interessant ist etwa die Erhebung zu dem Tatmittel „Internet".

Im Jahr 2021 wurden etwa acht Prozent der Straftaten mit dem Tatmittel „Internet" begangen.[9] Diese acht Prozent betreffen also grundsätzlich alle Arten von Straftaten wie etwa Diebstahl, Betrug und Beleidigungen. Acht Prozent klingt nun erst einmal nicht nach besonders viel, doch kam es hier in den letzten Jahren zu einem besorgniserregenden Anstieg. So wurden für 2021 zwar „nur" rund 380.000 Delikte registriert, die mittels des Tatmittels Internet begangen wurden – im Vergleich zum Vorjahr stellt dies jedoch ein Plus von fast 20% dar.[10] Für den Bereich der Beleidigungen ist sogar ein Zuwachs von 24% zu verzeichnen. In der Kategorie der „Cybercrime im engeren Sinne" wurden rund 124.137 Delikte registriert und auch insoweit kam es zu einem deutlichen Zuwachs von immerhin rund 15%.[11]

Zuwachs von fast 20% beim Tatmittel „Internet"

2. Was ist Cyberkriminalität?

Diese Zahlen und Begriffe führen unmittelbar zu der nächsten Frage: Was genau ist eigentlich mit „Cyberkriminalität" gemeint? Genügt es, dass das Internet als „Tatmittel" verwendet wird, oder existieren andere ausschlaggebende Aspekt dafür, dass eine Tat als Cyberkriminalität gilt?



Was sind ausschlaggebende Aspekte für die Klassifizierung als Cyberkriminalität?

9 Vgl. Bundeskriminalamt, PKS (2021), T 01 Grundtabelle – Fälle und T 05 Grundtabelle – Straftaten mit Tatmittel „Internet" – Fälle.

10 Vgl. Bundeskriminalamt, PKS (2020), T 05 Grundtabelle – Straftaten mit Tatmittel „Internet" – Fälle.

11 Bundeskriminalamt, Bundeslagebild Cybercrime (2021), S. 9.

Meistens hat man bezogen auf den Begriff der Cyberkriminalität eine ganze Menge Stichworte im Kopf, die in der medialen Berichterstattung, aber auch in einschlägigen Publikationen regelmäßig auftauchen. So ist etwa an den Einsatz von Schadsoftware (engl. Malware) zu denken, der in ganz verschiedenen Formen zur Begehung von Straftaten genutzt werden kann. Einen Unterfall stellt etwa die Ransomware dar, ein Verschlüsselungstrojaner, der die Daten auf einem PC verschlüsselt und hierüber die Erpressung des Nutzers bzw. der Nutzerin ermöglicht. Auch der Betrieb von Botnetzen, etwa zum Bitcoin Mining, der den Zusammenschluss einer Vielzahl von PCs voraussetzt – unbemerkt von den Nutzerinnen und Nutzern –, wird vielfach über Schadsoftware umgesetzt.

Vielfältige Einsatzbereiche für „Malware"

Ein weiteres Stichwort ist der digitale Hausfriedensbruch. Hierbei handelt es sich ebenfalls um einen Sammelbegriff, dem ganz unterschiedliche Angriffsarten unterfallen. Wird etwa im Falle der Ransomware eine Schadsoftware installiert, um Daten zu verschlüsseln und den Nutzer oder die Nutzerin im Anschluss zu erpressen, könnte man diesen Fall auch unter den Begriff des digitalen Hausfriedensbruchs fassen. Gleichzeitig gibt es andere Fälle, in denen es den Täterinnen und Tätern nicht um eine Erpressung geht, sondern etwa um eine gezielte Störung von kritischen Infrastrukturen und gegebenenfalls die Erlangung sensibler Daten. So wurde in der Vergangenheit beispielsweise der Deutsche Bundestag angegriffen.[12]

Beim Stichwort des „digitalen Hausfriedensbruchs" handelt es sich um einen Sammelbegriff für unterschiedliche Angriffsarten

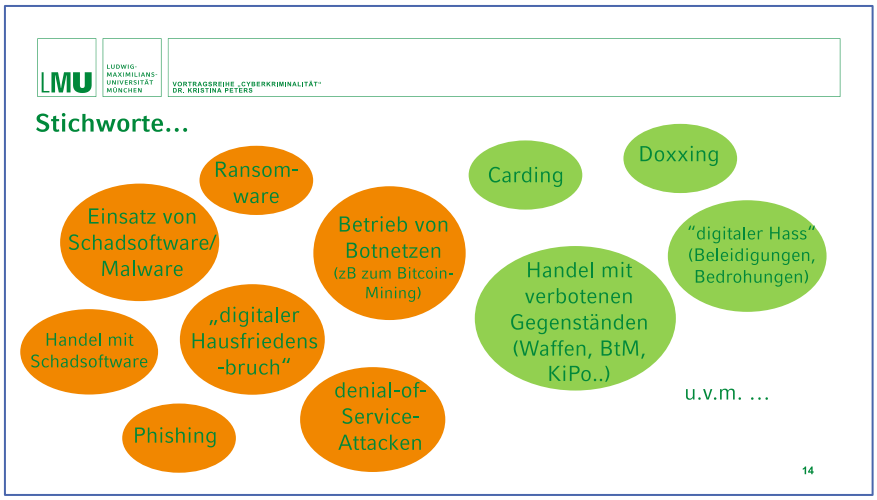
Weitere Stichworte, die den meisten mittlerweile bekannt sein dürften, sind etwa das Phishing oder Denial-of-Service-Attacken, das Carding (der Handel mit Kreditkartendaten) und das Doxing (das Zusammentragen und Veröffentlichten von personenbezogenen Daten). Ein wichtiger Phänomenbereich stellt außerdem der Handel mit verbotenen Gegenständen dar. Das können etwa Waffen, Betäubungsmittel, Kinderpornographie und vieles mehr sein. Dies wird oft im Zusammenhang mit Darknet-Plattformen thematisiert, ereignet sich aber durchaus auch häufig im Clearnet. Zuletzt existiert natürlich der große Bereich des digitalen Hasses – also Beleidigungen, Bedrohungen usw., die über das Internet verbreitet werden.

Ein wichtiger Phänomenbereich stellt der Handel mit verbotenen Gegenständen dar

Bezogen auf diese Phänomenbereiche hat sich ein differenziertes Begriffsregime herausgebildet: Die „Cybercrime im engen Sinne" bezeichnet Straftaten, die sich gegen das Internet, weitere Datennetze, informationstechnische Systeme oder deren Daten richten. Daneben tritt die

12 Netzpolitik.org, 19.06.15; Flade/ Tanriverdi, Hackerjagd mit Hindernissen, 22.4.21.

„Cybercrime im weiten Sinne“. Dies sind Straftaten, die unter der Nutzung des Tatmittels Internet begangen werden.[13] Anknüpfend an diese zwei Oberbegriffe lassen sich die genannten Phänomenbereiche aufteilen. Leitend ist dabei die Überlegung, ob eine Tat ausschließlich über das Internet oder andere Datennetze begangenen werden kann.



Grafik: links Cybercrime im engeren Sinne, rechts Cybercrime im weiten Sinne

Man unterscheidet zwischen Cybercrime im engeren und im weiteren Sinne

Hier interessiert vor allem die zweite Gruppe, die Cyberkriminalität im engen Sinne. Denn die Delikte der Cybercrime im weiten Sinne – beispielsweise den Handel mit verbotenen Gegenständen wie Waffen oder Betäubungsmittel – kannte man schon vor dem Internet und sie finden auch heute noch außerhalb des virtuellen Raumes statt. Gleiches gilt für Beleidigungen oder Bedrohungen. Werden solche Taten über das Internet begangen, so mag dies zum Teil erhebliche Schwierigkeiten mit sich bringen, gerade was die Verfolgbarkeit betrifft. Aber es handelt sich, anders als bei der Cybercrime im engen Sinne, nicht um neue Deliktsformen.

Nur bei Cybercrime im engen Sinne handelt es sich um neue Deliktsformen

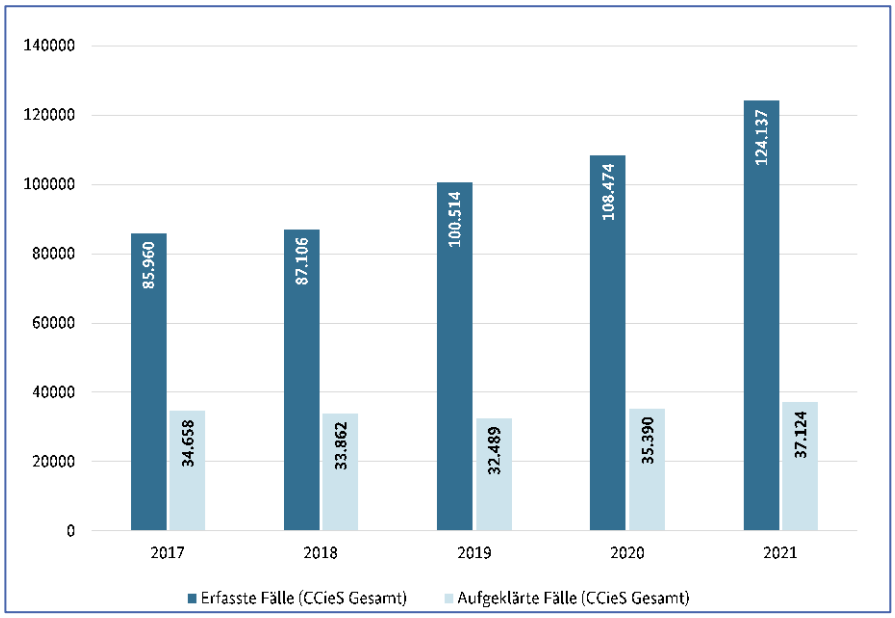
Das Bundeskriminalamt erstellt seit einiger Zeit jährlich ein eigenes Bundeslagebild zur Entwicklung der Cyberkriminalität.[14] Im Jahr 2021 wurden hier 124.137 Taten von Cybercrime im engen Sinne registriert. Das sind gerade einmal ungefähr drei Prozent aller begangenen Straftaten. Und doch ist auch hier die Tendenz steigend, wie die untenstehende Grafik zeigt. Die Aufklärungsquote lag im Jahr 2021 insgesamt bei rund 59%, bei den Delikten der Cybercrime im engen Sinne hingegen bei nur rund 30%.[15]

---

13 Zu den Begriffen siehe *Neubacher,* Kriminologie, 4. Aufl. 2020, Kapitel 26, Rn. 5; BKA, Bundeslagebild Cybercrime (2020), S. 42; das BKA verabschiedet sich allerdings ab dem Jahr 2022 von dieser Unterscheidung, siehe BKA, Bundeslagebild Cybercrime (2021), S. 4.

14 Bundeslagebild Cybercrime.

15 Vgl. Bundeskriminalamt, PKS (2021), T 01 Grundtabelle – Fälle.



Grafik: BKA, Bundeslagebild Cybercrime (2021), S. 5

Cybercrime im engen Sinne stellt drei Prozent aller begangenen Straftaten dar

Freilich liegt die Vermutung nahe, dass diese vergleichsweise niedrigen Zahlen – acht Prozent hinsichtlich des Tatmittels Internet, drei Prozent hinsichtlich der Cybercrime im engen Sinne – schlicht nicht die realen Zahlen abbilden und ein Großteil der Delikte gar nicht bekannt wird. Und auch wenn hierzu keine verlässlichen Aussagen möglich sind, so bleibt der bedenkenswerte Umstand bestehen, dass die Tendenz in beiden Bereichen eine deutlich steigende ist.

Vermutung: Ein Großteil der Delikte wird nicht bekannt

3. Zwischenfazit

Vor diesem Hintergrund ergibt sich bezogen auf die Ausgangsfrage, ob Cybercrime ein Modethema oder eine echte Bedrohung darstellt, eine differenzierte Antwort. Sehr viele klassische Delikte können mit dem Tatmittel Internet begangen werden. Insoweit wird das Tatmittel Internet in Zukunft wahrscheinlich eine noch größere und immer größer werdende Rolle spielen. Hierbei handelt es sich jedoch „nur“ um die Cybercrime im weiten Sinne, weil im Wesentlichen altbekannte Deliktformen betroffen sind. Die Lage scheint jedenfalls bislang nicht dramatisch zu sein. Freilich kann man – wie bei allen Delikten – nicht sicher sein, wie das Dunkelfeld genau aussieht. Daneben haben sich neue Deliktarten herausgebildet: die sogenannte Cybercrime im engen Sinne. Auch hier gilt, dass die Lage bislang nicht dramatisch zu sein scheint. Aber auch hier ist die Tendenz steigend und aller Wahrscheinlichkeit

Differenzierte Antwort auf die Ausgangsfrage

nach existiert ein nicht zu verachtendes Dunkelfeld, das teilweise immerhin auf bis zu 92% geschätzt wird.[16] Cyberkriminalität ist damit einerseits in einem gewissen Maße durchaus ein Modethema, weil oft diffuse Bedrohungsszenarien gezeichnet werden, denen man sich allzu schnell ausgeliefert fühlt. Gleichzeitig lässt sich festhalten, dass es sich schon vor dem Hintergrund des rasanten Anstiegs von Fallzahlen um eine durchaus ernstzunehmende Bedrohung handelt, die kontinuierlich zunimmt.

III. Cybercrime im engen (eigentlichen) Sinne: Was ist strafbar?

Damit kommen wir zum Schwerpunkt dieses Beitrags: Im Folgenden werden einige Phänomenbereiche der Cyberkriminalität im engen Sinne vorgestellt und die Frage beantwortet, was hier genau strafbar ist – und was nicht. Häufig macht die Befassung mit Cyberkriminalität stattdessen bei dieser Phänomenbeschreibung Halt. Es wird also beschrieben, was es alles gibt: Imposante Fachtermini mit noch imposanterer Technik, die dahintersteht – DDos-Attacken, Ransomware, Darknet. Da kann das Gefühl aufkommen, hilflos einer Übermacht von technikaffinen Personen gegenüberzustehen, denen man kaum etwas entgegenzusetzen hat. Stattdessen soll im Folgenden jedoch präzise dargestellt werden, was das geltende Recht eigentlich hierzu zu sagen hat.

Was hat das geltende Recht der Cyberkriminalität entgegenzusetzen?

Ein eindrückliches Beispiel, um das derzeitige Strafbarkeitsniveau zu illustrieren, ist der Einsatz von Ransomware. Den meisten dürfte die Vorgehensweise bereits bekannt sein, deshalb sollen hier nur die wesentlichen Punkte kurz ins Bewusstsein gehoben werden: Ein Computer lädt eine Schadsoftware; dies wird häufig unwissentlich durch den Nutzer oder die Nutzerin selbst veranlasst. Daraufhin werden die Dateien auf dem Computer und gegebenenfalls in dem ganzen System, das mit dem Computer verbunden ist, verschlüsselt. Es folgt eine Lösegeldforderung für die Freigabe dieser Daten. Daher der Begriff „Ransomware“: Der englische Begriff für Lösegeld („ransom“) wird mit dem Begriff „software“ kombiniert. In den letzten Jahren war ein starker Anstieg derartiger Fälle zu beobachten.[17] Diese Entwicklung hängt eng mit der zunehmenden Etablierung von Kryptowährung zusammen, durch

Starker Anstieg von Ransomware-Angriffen

[16] *Dreißigacker/von Skarczinski/Wollinger*, Cyberangriffe gegen Unternehmen in Deutschland. KFN-Forschungsberichte Nr. 162; Bundeskriminalamt, Bundeslagebild Cybercrime (2021), S. 4.

[17] Bundeskriminalamt, Bundeslagebild Cybercrime (2021), S. 2 f.

die eine anonyme Bezahlung der Erpresserinnen und Erpresser deutlich erleichtert wurde.[18]

Besonderes Aufsehen hat ein Fall im Jahre 2020 erregt: Damals kam es zu einem Ransomware-Angriff auf das Universitätsklinikum in Düsseldorf.[19] Das System der Klinik wurde verschlüsselt – und am Ende war ein Mensch tot. Dieser Fall soll hier als Beispiel dienen, um das aktuelle Kriminalisierungsniveau zu beschreiben. Dabei hat zu Beginn der Frage nach der Strafbarkeit immer – und dies wird leider häufig vernachlässigt oder lässt sich nicht ausreichend aufklären – die präzise Aufarbeitung der genauen technischenAbläufe zu stehen. Es wird sich noch zeigen, wie wichtig deren Kenntnis für die Beurteilung des exakten Strafbarkeitsniveaus ist. Weiß man nicht, was technisch passiert ist, dann weiß man auch nicht, wie dies rechtlich eingefangen werden kann.

Ransomware-Angriff auf das Universitätsklinikum Düsseldorf im Jahr 2020

Das Universitätsklinikum Düsseldorf ist eines der größten Krankenhäuser in Nordrhein-Westfalen, das jedes Jahr hunderttausende Patienten versorgt und im Jahr 2020 ein wichtiges Versorgungszentrum für Covid-19-Patientinnen und -patienten war. Die Steuerung der meisten Klinikabläufe – von den Türmechanismen über die Patientenakten bis zu der Durchführung von Operationen – erfolgt über rund 7.000 Computer, die über ein Netzwerk miteinander verbunden sind.[20] Im Dezember 2019 hatte ein Unternehmen, das eine Software vertreibt, die auch das Klinikum nutzte, vor einer Sicherheitslücke gewarnt. Bereits Anfang 2020 wurden weltweit Unternehmen attackiert, weil sich diese Information verbreitet hatte. Am 19. Januar 2020 wurde schließlich ein Update bereitgestellt, das diese Sicherheitslücke schloss. Der Zeitraum, bis dieses Update in Düsseldorf installiert wurde, betrug acht Tage. In der Zwischenzeit wurde allerdings bereits ein digitaler Zugang in die Klinik gelegt und eine Schadsoftware eingeschmuggelt. Im September 2020 schlugen die Erpresserinnen und Erpresser zu: Alle Daten wurden verschlüsselt und ein Lösegeld für die Freigabe des Systems gefordert sowie anderenfalls die Veröffentlichung sensibler Daten angedroht.

Es wurden Daten verschlüsselt, Lösegeld gefordert und die Veröffentlichung sensibler Daten angedroht

Als unmittelbare Konsequenz konnte niemand mehr auf das zentrale Computersystem zugreifen. Dieses enthielt Namen, Befunde, Laborergebnisse, Röntgenbilder, Dosierungen von Medikamenten und damit letztlich alles, was für den ordnungsgemäßen Betrieb des Klinikums er-

18 Ein weiterer aktueller Fall ist die Erpressung von Mediamarkt/Saturn Ende 2021, Spiegel Online vom 8.11.21.

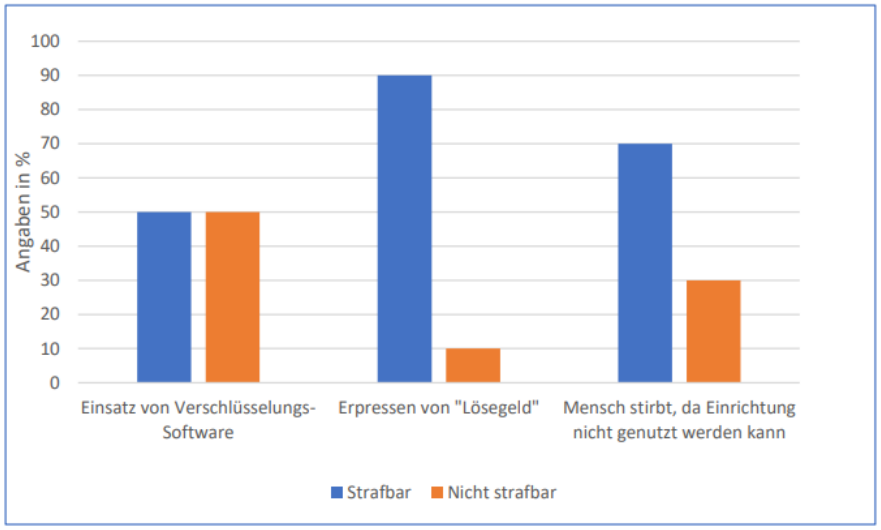
19 Zeit Online, vom 17.9.20; Uniklinik Düsseldorf, vom 17.9.20.

20 Eine detaillierte Beschreibung der Abläufe im Klinikum vor und nach dem Angriff bieten *Biermann/Middelhoff/Sehl* in Zeit Nr. 52/2020.

forderlich war. Die mittelbaren Konsequenzen waren vielfältig: Operationen mussten abgesagt werden – unter anderem, weil OP-Anweisungen nur digital verfügbar waren. In Papierform wurden die Patientenakten nicht mehr vorrätig gehalten. Zum Teil mussten Patientinnen und Patienten daher mit Blick auf Medikamente und deren Dosierung „blind" behandelt werden. Zudem musste die Notaufnahme geschlossen und Rettungswagen auf andere Kliniken umverteilt werden. Eine Frau mit Herzbeschwerden wurde in der Folge statt nach Düsseldorf nach Wuppertal gefahren, sodass sie eine Stunde später behandelt wurde – und verstarb. Im Übrigen entstanden dem Klinikum selbstverständlich hohe Kosten: Das System musste nach dem Angriff komplett neu eingerichtet werden und es dauerte 13 Tage, bis allein die Notaufnahme wieder einsatzbereit war. Insgesamt hatte der Angriff also über die Verschlüsselung hinaus erhebliche mittelbare Konsequenzen.

> Eine Frau mit Herzbeschwerden wurde verspätet behandelt und verstarb

Inwieweit ist dieses Geschehen nun strafrechtlich relevant? Dies betrifft im Wesentlichen drei Punkte: Erstens den Einsatz der Verschlüsselungssoftware, zweitens die Lösegeldforderung und drittens den Umstand, dass ein Mensch nicht in die Notaufnahme gebracht werden konnte und verstarb.



Grafik: Umfrageergebnisse aus der Vortragsreihe zu der Frage, welche Handlungen strafbar sind

> Welche Handlungen sind nach aktuellem Recht strafbar?

1. Einsatz der Verschlüsselungssoftware

Die größte Unsicherheit besteht regelmäßig hinsichtlich des Einsatzes der Verschlüsselungssoftware. Dabei handelt es sich tatsächlich um den in rechtlicher Hinsicht kompliziertesten Aspekt derartiger Fallkonstellationen. Betroffen sind die sogenannten Datendelikte des Strafgesetzbuchs. Wirft man lediglich einen flüchtigen Blick auf diese Delikte, kann

der Eindruck entstehen, diese seien recht unsystematisch über das Strafgesetzbuch verstreut. Sieht man jedoch genauer hin, erkennt man, dass das nicht stimmt: Beim Schaffen der Tatbestände hat die Gesetzgebung sich vielmehr bemüht, diese in die bestehende Struktur des Strafgesetzbuchs einzufügen. Es wurde also nach bereits existierenden Tatbeständen gesucht, zu denen die neuen Tatbestände „passen".

Verletzung des persönlichen Lebens- und Geheimbereichs (§§ 201-210 StGB)

Zunächst lohnt ein Blick in den 15. Abschnitt des Besonderen Teils des Strafgesetzbuchs: Die Verletzung des persönlichen Lebens- und Geheimbereichs (§§ 201-210 StGB). Diese Normen zielen auf den persönlichen Geheimnisschutz und beinhalten beispielsweise einen Tatbestand der Verletzung des Briefgeheimnisses (§ 202 StGB). Es lag nahe, hier auch solche Datendelikte zu verankern, die von ihrer Schutzrichtung her zu diesem Abschnitt passen. Ein Beispiel ist das Ausspähen von Daten in § 202a StGB; daneben finden sich die Tatbestände des Abfangens von Daten (§ 202b StGB), des Vorbereitens, des Ausspähens und Abfangens von Daten (§ 202c StGB) sowie der Datenhehlerei (§ 202d StGB). Daneben ist vor allem der 27. Abschnitt interessant, der mit „Sachbeschädigung" überschrieben ist und die §§ 303-305a StGB umfasst. Der Abschnitt zielt in erster Linie auf den Eigentumsschutz. Dieser Leitgedanke lässt sich auf den Umgang mit Daten übertragen, indem man auf deren Verwendbarkeit – also den Zugriff und die Nutzbarkeit – abstellt.[21] In diesem Abschnitt wurde in Anlehnung an die Sachbeschädigung (§ 303 StGB) die Tatbestände der Datenveränderung (§ 303a StGB) sowie der Computersabotage (§ 303b StGB) geschaffen. Zu unterscheiden sind also das Anliegen des Geheimnisschutzes – ich will nicht, dass jemand meine Daten *kennt* – und das Äquivalent zu einem Eigentumsschutz – ich möchte bitte meine Daten *behalten*. Sind die betroffenen Daten darüber hinaus beweiserheblich, kommen zudem noch Tatbestände im Rahmen der Urkundendelikte in Betracht.[22] Die Datendelikte sind mithin keineswegs willkürlich über das Strafgesetzbuch verstreut. Ausschlaggebend ist vielmehr der jeweilige Schutzzweck.

Sachbeschädigung (§§ 303-305a StGB)

Bezogen auf den Fall des Düsseldorfer Universitätsklinikums ist zunächst das Ausspähen von Daten interessant. Hierzu heißt es in § 202a StGB: „Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders

[21] Bundestag Drucksache 10/5058, S. 34; BayObLGSt 1993, 86, 88; *Wieck-Noodt,* in: MüKo-StGB, Bd. 5, 3. Aufl. 2019, § 303a Rn. 2; *Hecker*, in: Schönke/Schröder-StGB, 30.Aufl. 2019, § 303a Rn. 1; *Zaczyk,* in: NK-StGB, 5. Aufl. 2017, § 303a Rn. 2.

[22] Es kommen insbesondere § 269 StGB (Fälschung beweiserheblicher Daten) und § 274 Abs. 1 Nr. 2 StGB (Urkundenunterdrückung) in Betracht.

gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft." Das Vorgehen der Erpresserinnen oder Erpresser im Düsseldorfer Fall lässt sich hierunter leicht subsumieren: Die betroffenen Dateien, die verschlüsselt wurden, sind Daten. Sie sind auch nicht für die Täterinnen bzw. Täter bestimmt und gegen unberechtigten Zugang besonders gesichert (insoweit wird man davon ausgehen können, dass sie durch eine Firewall oder Ähnliches geschützt waren). Damit wurde hier auch eine Zugangssicherung überwunden: Die Schadsoftware wurde eingeschmuggelt und es wurde ein Zugang gelegt – ein Gericht müsste insoweit freilich feststellen, wie dieses System genau gesichert war. Da die handelnden Personen mit der Veröffentlichung sensibler Daten gedroht haben, werden sie wohl auch an die Daten gelangt sein – auch das müsste freilich in einem Strafverfahren genauer aufgeklärt werden. Insgesamt dürften an einer Strafbarkeit gemäß § 202a StGB jedoch wenig Zweifel bestehen.

Düsseldorfer Fall: Strafbarkeit gemäß § 202a StGB kaum zweifelhaft.

Daneben kommt die Datenveränderung in § 303a StGB in Betracht: „Wer Daten löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft." Diese Tathandlungen sind leider etwas schwerer zu greifen und insbesondere schwer voneinander abzugrenzen. Sicher ist jedenfalls, dass im Düsseldorfer Fall Daten unterdrückt wurden, das heißt, dem Zugriff für einen nicht unerheblichen Zeitraum entzogen waren.[23] Daneben wurden sie wohl auch unbrauchbar gemacht, weil sie infolge der Verschlüsselung nicht mehr ordnungsgemäß verwendet werden konnten.[24] Auch könnte man das Verschlüsseln als eine Veränderung ansehen, die vorliegen soll, wenn es zu einer inhaltlichen Umgestaltung kommt.[25] Es kommen also mehrere Tathandlungen in Betracht, wobei jedenfalls ein Unterdrücken vorliegt.[26]

Hinsichtlich der Datenveränderung in § 303a StGB ist jedenfalls ein Unterdrücken zu bejahen

Wirklich interessant ist dann aber der Blick auf den Tatbestand der Computersabotage in § 303b StGB, der das Strafmaß massiv in die Höhe treibt. Hierbei handelt es sich um einen recht komplexen Tatbestand mit vielen Varianten. Vorliegend kommen vor allem § 303b Absatz 1, 2 und 4 StGB in Betracht. Absatz 1 sieht zunächst ein Strafmaß

§ 303b StGB lässt das Strafmaß massiv ansteigen.

23 Bundestag Drucksache 10/5058, S. 34 f.; *Hecker*, in: Schönke/Schröder-StGB, 30. Aufl. 2019, § 303a Rn. 6.

24 Bundestag Drucksache 10/5058, S. 35; *Hecker*, in: Schönke/Schröder-StGB, 30. Aufl. 2019, § 303a Rn. 7.

25 Bundestag Drucksache 10/5058, S. 35; *Hecker*, in: Schönke/Schröder-StGB, 30. Aufl. 2019, § 303a Rn. 8.

26 Werden mehrere Tathandlungsalternativen gleichzeitig verwirklicht, liegt im Übrigen nur eine Tat vor, *Wieck-Noodt*, in: MüKo-StGB, Bd. 5, 3. Aufl. 2019, § 303a Rn. 24.

von bis zu drei Jahren Freiheitsstrafe vor. Vorausgesetzt ist eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, was Bagatellfälle ausschließen soll.[27] Diese Datenverarbeitung muss erheblich gestört werden und zwar dadurch, dass eine Tat nach Nummer 1, 2 oder 3 begangen wird. § 303b Absatz 1 Nr. 1 StGB verweist dabei direkt auf § 303a StGB – es handelt sich insoweit um eine Qualifikation zu § 303a StGB.[28] Eine erhebliche Störung dürfte hier vorliegen, da das System komplett verschlüsselt wurde. Laufen – etwa im Rahmen eines Botnetzes – lediglich verborgen im Hintergrund Rechenoperationen, die die Nutzung des Geräts nicht erheblich beeinträchtigen, wären insoweit Zweifel angezeigt, doch ist im vorliegenden Fall die Erheblichkeitsschwelle in jedem Fall überschritten. Darüber hinaus kommt § 303b Absatz 1 Nr. 2 StGB in Betracht: Das Eingeben oder Übermitteln von Daten mit Nachteilszufügungsabsicht. Wird wie hier etwas in das System eingeschmuggelt, dürfte diese Variante ebenfalls erfüllt sein.[29] Absatz 1 Nr. 3 ist hingegen sehr eng an die Sachbeschädigung in § 303 StGB angelehnt und stellt darauf ab, dass physisch etwas mit einer Datenverarbeitungsanlage oder einem Datenträger passiert.[30]

Des Weiteren kommt § 303b Absatz 2 StGB in Betracht, der das Strafmaß auf Freiheitsstrafe bis zu fünf Jahre oder Geldstrafe erhöht, wenn es sich um eine Datenverarbeitung handelt, die für einen fremden Betrieb, ein fremdes Unternehmen oder für eine Behörde von wesentlicher Bedeutung ist. Das Universitätsklinikum gilt als fremdes – öffentliches – Unternehmen.[31] Ein weiteres Mal gesteigert wird das Strafmaß durch Absatz 4, der in besonders schweren Fällen des Absatzes 2 die Strafe auf Freiheitsstrafe von sechs Monaten bis zu 10 Jahren erhöht. Hier wird also eine Freiheitsstrafe zwingend angeordnet – ein doch erhebliches Strafmaß für einen Straftatbestand, der in der Nähe der Sachbeschädigung steht. Ein solcher besonders schwerer Fall liegt vor, wenn der Täter bzw. die Täterin (1) einen Vermögensverlust großen Ausmaßes herbeiführt, (2) gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Computersabotage verbunden hat, oder (3) durch die Tat die Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder die Sicherheit der Bundesrepublik Deutschland beeinträchtigt. Letzteres wird bei einem

§ 303b Absatz 4 StGB: Freiheitsstrafe von sechs Monaten bis zu 10 Jahren.

[27] Bundestag Drucksache 16/3656, S. 13; bei geschädigten Privatpersonen wird vorausgesetzt, dass die Datenverarbeitung für die Lebensgestaltung dieser Person eine zentrale Funktion einnimmt; *Wieck-Noodt*, in: MüKo-StGB, Bd. 5, 3. Aufl. 2019, §303b Rn. 9.

[28] *Hecker*, in: Schönke/Schröder-StGB, 30. Aufl. 2019, §303b Rn. 6.

[29] *Weidemann*, in: BeckOK-StGB, 53. Ed. 2022, § 303b Rn. 11.

[30] *Hecker*, in: Schönke/Schöder-StGB, 30. Aufl. 2019, § 303b Rn. 8; *Weidemann*, in: BeckOK-StGB, 53. Ed. 2022, § 303b Rn. 14.

[31] *Hecker*, in: Schönke/Schröder-StGB, 30. Aufl. 2019, § 303b Rn. 12.

Universitätsklinikum zu bejahen sein. Häufig sind bei Ransomware-Erpressungen zudem Banden betroffen und auch die Gewerbsmäßigkeit ist oft zu bejahen. Im Übrigen wäre wohl auch ein Vermögensverlust großen Ausmaßes – die Grenze wird hier bei ungefähr bei 50.000€ angesetzt[32] – schon mit Blick auf die Kosten für die Systemerneuerung einschlägig. Damit würde im Ergebnis allein für die Verschlüsselung des Systems bereits eine zwingende Freiheitsstrafe von sechs Monaten bis zu 10 Jahren drohen.

Ein Tatbestand, der bis hierher noch überhaupt keine Rolle gespielt hat, aber immer wieder Thema ist, wenn es um Cyberkriminalität geht, ist der sogenannte „Hackerparagraph" in § 202c StGB. Dieser betrifft das Vorbereiten des Ausspähens und Abfangens von Daten. Es handelt sich um einen Vorbereitungstatbestand, der insbesondere darauf abzielt, dass bestimmte Computerprogramme hergestellt oder sich verschafft oder verkauft werden, um eine Straftat gemäß § 202a StGB oder § 202b StGB vorzubereiten. Weil sich in §§ 303a, b StGB Verweisungen finden, greift § 202c StGB ebenfalls, wenn die Vorbereitung dieser Delikte betroffen ist. Weil es sich aber bloß um einen Vorbereitungstatbestand handelt, ist dieser nicht relevant, wenn das vorbereitete Delikt tatsächlich begangen wird – dann ist der § 202c StGB bloße mitbestrafte Vortat.[33] Der Unrechtsgehalt dieser Vorbereitungshandlung geht in diesen Fällen in der Begehung des eigentlichen Straftatbestands – also der Tat, um die es eigentlich geht – auf. § 202c StGB kommt dann nur noch mit Blick auf etwaige Personen im Hintergrund in Betracht, die an der eigentlichen Tat nicht beteiligt waren und zum Beispiel die Ransomware entwickelt haben.

Der sog. „Hackerparagraph" in § 202c StGB kriminalisiert nur Vorbereitungshandlungen

2. Die Lösegeldforderung

Hinsichtlich der Lösegeldforderung kann auf den „klassischen" Tatbestand der Erpressung in § 253 StGB abgestellt werden, der unabhängig davon eingreift, ob eine Erpressung in der analogen oder in der digitalen Welt begangen wird. Hiernach gilt: „Wer einen Menschen rechtswidrig mit Gewalt oder durch Drohung mit einem empfindlichen Übel zu einer Handlung, Duldung oder Unterlassung nötigt und dadurch dem Vermögen des Genötigten oder eines anderen Nachteil zufügt, um sich oder einen Dritten zu Unrecht zu bereichern, wird mit Freiheitsstrafe

Die Erpressung in § 253 StGB greift unabhängig davon, ob Handlungen in der analogen oder digitalen Welt begangen werden

[32] Bei der Auslegung des Vermögensverlusts großen Ausmaßes, kann die Auslegung des § 263 StGB zugrunde gelegt werden, *Weidemann*, in: Beck-OK/StGB, 53. Ed. 2022, § 303b Rn. 27; danach liegt ein Vermögensverlust großen Ausmaßes bei einem Wert von mindestens 50.000 € vor, BGH, Urteil vom 7.10.2003 – 1 StR 274/03, NJW 2004, 169.

[33] *Eisele*, in: Schönke/Schröder-StGB, 30. Aufl. 2019, § 202c Rn. 10.

bis zu fünf Jahren oder mit Geldstrafe bestraft."[34] Insoweit ist die Subsumtion recht unproblematisch: Den verantwortlichen Personen im Uni-Klinikum wurde in Aussicht gestellt, die Übersendung des Entschlüsselungscodes zu unterlassen. Hierbei handelt es sich in Anbetracht der massiven Einschränkungen offenkundig um einen Nachteil, hinsichtlich dessen nicht erwartet werden kann, dass dem in besonnener Selbstbehauptung standgehalten wird.[35] Da die Verschlüsselung eines fremden Computersystems, wie insbesondere die §§ 303a, b StGB deutlich machen, rechtswidrig ist, ist das hierin liegende Unterlassen ebenfalls als rechtswidrig einzuordnen. Das Uni-Klinikum hatte mithin einen Anspruch auf die Übersendung des Entschlüsselungscodes, sodass dem Unterlassen der Charakter eines Übels zukommt, mit dem gedroht wird. Da die Erpressung einen „Nötigungserfolg" voraussetzt, wäre das Delikt indes nur vollendet, wenn das Lösegeld auch bezahlt wird. Ansonsten liegt lediglich ein Versuch gemäß §§ 253 Absatz 3, 22, 23 StGB vor. Im Übrigen käme hier ein besonders schwerer Fall in Betracht: Einen solchen sieht § 253 Absatz 4 StGB für gewerbsmäßige oder Bandentaten vor, sodass das oben Gesagte entsprechend gilt. In diesem Fall läge das Strafmaß bei Freiheitsstrafe nicht unter einem Jahr.[36]

Der „Nötigungserfolg" tritt nur ein, wenn das Lösegeld auch bezahlt wird – ansonsten liegt ein Versuch vor

3. Tod eines Menschen

Zuletzt gilt es, einen Blick auf die Tötungsdelikte zu werfen. In Betracht kommen hier Totschlag (§ 212 StGB) und Mord (§ 211 StGB)[37] zu Lasten der verstorbenen Patientin. Hierzu müsste die Verschlüsselung kausal für den Tod gewesen sein. Kausal ist ein Verhalten, das nicht hinweggedacht werden kann, ohne dass der Erfolg in seiner konkreten Gestalt entfiele (conditio-sine-qua-non-Formel). Wäre das Computersystem nicht verschlüsselt worden, wäre die Notaufnahme nicht geschlossen, die Patientin in das Uni-Klinikum in Düsseldorf transportiert und

War die Verschlüsselung kausal für den Tod der Patientin?

---

34 Zum Tatbestand der Erpressung allgemein *Rengier*, Strafrecht Besonderer Teil I, 24. Aufl. 2022, § 11 Rn. 1 ff.; *Wessels/Hillenkamp/Schuhr*, Strafrecht Besonderer Teil 2, 44. Aufl. 2021, § 18.

35 *Rengier*, Strafrecht Besonderer Teil II, 23. Aufl. 2022, § 23 Rn. 44; *Wessels/Hettinger/Engländer*, Strafrecht Besonderer Teil 1, 45. Aufl. 2021, Rn. 369.

36 Im Übrigen wäre auch an § 255 StGB zu denken.

37 Es wäre verfehlt, den Schwerpunkt auf ein Unterlassen (der Herausgabe des Entschlüsselungscodes) zu legen. Sowohl nach dem Energiekriterium als auch nach einer normativen Betrachtungsweise ist hier auf die Verschlüsselung des Systems abzustellen; zur Abgrenzung von Tun und Unterlassen siehe *Rengier*, Strafrecht Allgemeiner Teil, 13. Aufl. 2021, § 48 Rn. 8 ff.; Wessels/Beulke/Satzger, Strafrecht Allgemeiner Teil, 51. Aufl. 2021, Rn. 428 f.; ausführlich zu den Tötungsdelikten *Rengier,* Strafrecht Besonderer Teil II, 23. Aufl. 2022, § 3 Rn. 1 ff.; *Wessels/Hettinger/Engländer*, Strafrecht Besonderer Teil 1, 45. Aufl. 2021, § 2.

früher behandelt worden.[38] Eine Strafbarkeit hinge hier davon ab, ob das Gericht zu dem Schluss kommt, dass die Patientin in diesem Fall überlebt hätte.

Sofern dies festgestellt werden kann, wäre die objektive Zurechnung unproblematisch:[39] Die Verschlüsselung des Computersystems einer Klinik, auf dem sämtliche Patientendaten gespeichert sind, beinhaltet ersichtlich die Gefahr, dass Patientinnen und Patienten nicht mehr adäquat behandelt werden können, da die relevanten Informationen fehlen. Auch wird hiermit die Gefahr gesetzt, dass die Abläufe der Klinik zum Erliegen kommen und wichtige Einrichtungen wie die Notaufnahme geschlossen werden müssen. Genau diese Gefahr hat sich in dem Tod der Patientin realisiert: Ein Zurechnungsausschluss infolge eines atypischen Kausalverlaufs kommt insoweit nicht in Betracht. Ein solcher liegt vor, wenn der Kausalverlauf so sehr außerhalb der Lebenserfahrung liegt, dass mit ihm vernünftigerweise nicht gerechnet zu werden braucht. Jedoch ist durchaus absehbar, dass die verantwortlichen Personen infolge der Probleme zu verhindern versuchen, dass weitere Personen aufgenommen und einer entsprechenden Gefährdung ausgesetzt werden, und daher die Notaufnahme schließen. Naheliegend ist damit auch, dass Notfälle in weiter entfernte Krankenhäuser transportiert werden müssen und infolge einer verspäteten Behandlung versterben können. Auch ein Zurechnungsausschluss infolge eines eigenverantwortlichen Dazwischentretens Dritter kommt hier mit Blick auf die Anweisung an die Rettungswagen, verletzte Personen in andere Krankenhäuser zu transportieren, nicht in Betracht: Diese Anweisung knüpfte unmittelbar an die Verschlüsselung des Computersystems an und versuchte, die hierdurch geschaffene Gefahr – dass Notfälle nicht adäquat versorgt werden können – abzuwehren. Bei wertender Betrachtung ist mithin die mit Blick auf die längeren Transportwege entstandene Gefahr keine neue Gefahr, sondern immer noch dem Handeln der Täterinnen oder Täter als ihr „Werk" zuzurechnen. Eine Strafbarkeit würde daher nur noch vom subjektiven Tatbestand und damit davon abhängen, welches konkrete Vorstellungsbild diese hatten. Wer jedoch ein Krankenhaus angreifen will, indem das komplette Computersystem verschlüsselt wird, bei dem liegt es nahe, dass etwaige Personenschäden billigend in Kauf genommen werden.

Die objektive Zurechnung dürfte zu bejahen sein.

[38] Die Entscheidung Dritter zur Abweisung der Rettungswagen berührt die Kausalität nicht (Fall der sog. fortwirkende Kausalität); zur Kausalität siehe *Rengier*, Strafrecht Allgemeiner Teil, 13. Aufl. 2021, § 13; Wessels/Beulke/Satzger, Strafrecht Allgemeiner Teil, 51. Aufl. 2021, Rn. 225 f.

[39] Zur objektiven Zurechnung siehe *Rengier*, Strafrecht Allgemeiner Teil, 13. Aufl. 2021, § 13; Wessels/Beulke/Satzger, Strafrecht Allgemeiner Teil, 51. Aufl. 2021, Rn. 253 f.

In diesem Fall käme im Übrigen auch ein Mord (§ 211 StGB) in Betracht. Zunächst liegt eine Verwendung „gemeingefährlicher Mittel" nahe: Gemeingefährlich sind Tatmittel, die der Täter oder die Täterin in der konkreten Tatsituation nicht sicher zu beherrschen vermag, so dass ihr Einsatz geeignet ist, über das oder die ausersehenen Opfer hinaus das Leben einer Mehrzahl unbeteiligter Dritter zu gefährden.[40] Von einer „Mehrzahl" wird überwiegend jedenfalls bei mindestens drei Personen ausgegangen. Die vollständige Verschlüsselung eines Computersystems erscheint insoweit gewissermaßen als eine „digitale Bombe", die auf das Krankenhaus einschließlich der Intensivstation „geworfen" wird.[41] Darüber hinaus kommen mit Blick auf das Lösegeld die Mordmerkmale der Habgier[42] und der Ermöglichungsabsicht[43] in Betracht. Im Übrigen wäre auch an eine Versuchsstrafbarkeit hinsichtlich der übrigen Patientinnen und Patienten – jedenfalls, soweit sich diese etwa auf einer Intensivstation befanden – zu denken.

Die Verschlüsselung gleicht einer „digitalen Bombe"

4. Der Düsseldorfer Fall: Ein folgenschwerer Irrtum

Im Fall des Düsseldorfer Klinikums ergaben die Ermittlungen allerdings eine Überraschung: Die Polizei fand heraus, dass das Klinikum lediglich versehentlich getroffen wurde – eigentlich wollte man die Düsseldorfer Universität angreifen. Nachdem der Fehler aufgeklärt wurde, wurde ein Entschlüsselungscode bereitgestellt, ohne dass ein Lösegeld gezahlt wurde. Die Obduktion der verstorbenen Patientin ergab zudem, dass diese auch nicht hätte gerettet werden können, wenn sie in das Düsseldorfer Klinikum transportiert worden wäre. Die weiteren Ermittlungen der Behörden gestalten sich dem Vernehmen nach schwierig

Das Klinikum wurde lediglich versehentlich getroffen

---

40 *Rengier,* Besonderer Teil II, 23. Aufl. 2022, § 4 Rn. 96; *Wessels/Hettinger/Engländer*, Strafrecht Besonderer Teil 1, 45. Aufl. 2021, Rn. 57.

41 Zu dem Streit, ob Gemeingefährlichkeit vorliegt, wenn das Tötungsmittel zwar eine Mehrzahl von Menschen gefährdet, während gleichzeitig der Tod dieser Menschen von dem (Eventual-)Vorsatz des Täters bzw. der Täterin umfasst ist, siehe *Rengier*, Besonderer Teil II, 23. Aufl. 2022, § 4 Rn. 101 f.; *Wessels/Hettinger/Engländer*, Strafrecht Besonderer Teil 1, 45. Aufl. 2021, Rn. 57; nach der vorzugswürdigen Repräsentantenlösung dürften die gemeingefährlichen Mittel hier zu bejahen sein.

42 Zum Mordmerkmal der Habgier *Rengier,* Besonderer Teil II, 23. Aufl. 2022, § 4 Rn. 24 ff.; *Wessels/Hettinger/Engländer*, Strafrecht Besonderer Teil 1, 45. Aufl. 2021, Rn. 48.

43 Zum Mordmerkmal der Ermöglichungs- und Verdeckungsabsicht *Rengier*, Besonderer Teil II, 23. Aufl. 2022, § 4 Rn. 106 ff.; *Wessels/Hettinger/Engländer*, Strafrecht Besonderer Teil 1, 45. Aufl. 2021, Rn. 73 f. Tötungshandlung und Erpressung fallen hier nicht in einem Akt zusammen, sodass es sich um eine „andere Tat" handelt. Eine Tötung, die dem Zweck dient, einer beabsichtigten erpresserischen Drohung Nachdruck zu verleihen, ist ein Standardfall der Ermöglichungsabsicht, siehe etwa *Rengier*, Besonderer Teil II, 23. Aufl. 2022, § 4 Rn. 111.

und dauern wohl noch an. Die Staatsanwaltschaft Köln hat nach Presseberichten Rechtshilfeersuchen an verschiedenen Staaten gerichtet.[44] Die Spuren der Tat scheinen nach Russland zu führen.[45]

5. Zusammenfassung

Cyberattacken können empfindlich treffen, sind aber gleichzeitig in vielerlei Hinsicht strafbar

Der Fall des Universitätsklinikums Düsseldorf illustriert anschaulich, wie empfindlich Cyberattacken treffen und wie schnell auch Menschenleben gefährdet sein können. Gleichzeitig haben die obigen Ausführungen dargelegt, dass das Strafgesetzbuch vielfältige Tatbestände aus dem Bereich des „klassischen" Strafrechts wie der Cyberkriminalität im engen Sinne bereithält, welche die einzelnen Schritte des „Geschäftsmodells Ransomware" kriminalisieren. Zum einen ist bereits die Verschlüsselung eines Computersystems strafbar, wobei die Einzelheiten von dem technischen Ablauf abhängen. Soweit hier Unsicherheiten im Rahmen der Auslegung der Datendelikte, insbesondere der hier thematisierten §§ 202a, 303a, 303b StGB bestehen, ist zu berücksichtigen, dass noch nicht allzu viel Rechtsprechung in diesem Bereich existiert. Interessant ist insoweit etwa eine Entscheidung aus April 2021, die ausführlich darlegt, welche technischen Abläufe im Einzelnen betroffen waren.[46]

Kommt es zu Vermögensschäden, wird dies von den herkömmlichen Straftatbeständen abgedeckt. Wird kausal, objektiv zurechenbar und vorsätzlich der Tod eines Menschen verursacht, kommen außerdem die Tötungsdelikte in Betracht. Der allgemeine Teil des Strafgesetzbuchs hilft hier bei typischen Modifikationen: Bei mehreren Täterinnen bzw. Tätern kommt insbesondere die Mittäterschaft (§ 25 Abs. 2 StGB) in Betracht; ansonsten ist an Anstiftung (§ 26 StGB) oder Beihilfe (§ 27 StGB) zu denken. Bei einem typischen Ransomware-Fall, bei dem das Opfer infolge einer Täuschung selbst die Schadsoftware herunterlädt, läge zudem ein Fall der mittelbaren Täterschaft vor (§ 25 Abs. 1 Alt. 2 StGB), bei dem das Opfer als „Werkzeug gegen sich selbst" eingesetzt wird.

IV. Besteht Handlungsbedarf?

Freilich darf nicht übersehen werden, dass eine Bestrafung in vielen Fällen an einer gelingenden Strafverfolgung scheitern wird – möglicher-

44 Sueddeutsche.de vom 3.9.2021.
45 Spiegel.de vom 22.9.2020.
46 BGH, Beschluss vom 8.4.2021 – 1 StR 78/21, BeckRS 2021, 16213.

weise auch im Fall des Universitätsklinikums Düsseldorf. Die Strafverfolgung wird aber nicht dadurch effektiver, dass immer neue Straftatbestände geschaffen werden oder der Strafrahmen von Delikten angehoben wird. Wollte man die Strafverfolgung tatsächlich effektiver gestalten, bräuchte es in erster Linie mehr entsprechend ausgebildetes Personal, das die technischen Abläufe durchdringt, über entsprechend leistungsfähige Infrastruktur verfügt und so auf Augenhöhe gegen Täterinnen und Täter ermittelt. Hier anzusetzen ist allerdings mit Kosten verbunden – anders als die bloße Schaffung oder Verschärfung von Straftatbeständen.

Der Komplex der Cyberkriminalität ist durchaus besorgniserregend – man denke nur an das Beispiel einer Schadsoftware, die in einem Atomkraftwerk entdeckt wurde.[47] So zu tun, als würde Kriminalität sich nicht verändern, wäre gefährlich, und nicht auf neue Erscheinungsformen von kriminellem Handeln zu reagieren, kann keine Option sein. Jedoch sollte nicht verkannt werden, dass entsprechende Straftatbestände bereits existieren und der Handlungsbedarf damit nicht unbedingt auf Ebene des materiellen Rechts besteht: Die Tatbestände des Ausspähens von Daten in § 202a StGB, der Datenveränderung in § 303a StGB und der Computersabotage in § 303b StGB existieren bereits seit 1986.[48] Diese Tatbestände wurden im Laufe der Jahre modifiziert, und an neue Gegebenheiten angepasst, aber im Grundsatz existieren sie schon lange. Sie sind nicht perfekt und lassen insbesondere an vielen Stellen eine klare Beschreibung der Tatbestandshandlungen vermissen, aber sie sind da und man kann mit Ihnen arbeiten.

> Die Strafverfolgung wird nicht dadurch effektiver, dass neue Straftatbestände geschaffen werden

Insoweit gilt aber auch: Statt neue Straftatbestände zu schaffen, würde es sich vielmehr anbieten, punktuell überstürzte Maßnahmen rückgängig zu machen. Das wäre allerdings ein Thema für einen ganz eigenen Beitrag. Nur kurz erwähnt seien an dieser Stelle die Strafbarkeitsrisiken für sogenanntes ethisches Hacken und für die Sicherheitsberatung.[49] Bei der Datenhehlerei besteht zudem ein erhebliches Strafbarkeitsrisiko, wenn Daten öffentlich gemacht werden, die von Whistleblowern stammen.[50] Und bei der Datenveränderung fehlt ein Tatbestandsmerkmal,

> Statt neue Straftatbestände zu schaffen, würde es sich vielmehr anbieten, punktuell überstürzte Maßnahmen rückgängig zu machen

47 *Scherschel*, heise.de vom 24.6.2016.
48 Bundesgesetzblatt Teil I, 1986, Nr. 21 vom 23.05.1986.
49 Vorschlag für eine Entkriminalisierung bei *Klaas*, MMR 2022, 187.
50 Vorschläge für eine Entkriminalisierung insbesondere bzgl. einer Zusammenarbeit zwischen Whistleblowern und Journalisten bei *Buermeyer* auf netzpolitik.org; *Herfurth/Drews*, ZD-Aktuell 2017, 05490; eine kriminalpolitische Einschätzung liefert auch *Kargl*, in: NK-StGB, 5. Aufl. 2017, § 202d Rn. 18.

das eine Fremdheit der Daten voraussetzt.[51] Schon wegen der sich hieraus ergebenden Unbestimmtheit wird der Tatbestand von einigen für verfassungswidrig gehalten.[52] Auch sonst bestehen viele kleinere dogmatische Unklarheiten: Überflüssige Tatbestandmerkmale, fehlende Tatbestandsmerkmale, unbestimmte Tatbestandsmerkmale. Dies sind typische Zeichen von Straftatbeständen, die aus einer politischen Überstürzung heraus geschaffen werden und für die man sich nicht genug Zeit genommen hat, um sie so abzufassen, dass sie die Anforderungen an ein ausreichend bestimmtes Strafrecht erfüllen.

V. Fazit

Um zu der Ausgangsfrage zurückzukehren, ob das Strafrecht in seiner aktuellen Kodifizierung die rasanten Entwicklungen im Bereich der Cyberkriminalität noch abdecken kann oder es neue Straftatbestände braucht: Das Fazit dieses Beitrags lautet, dass das Strafrecht insoweit ganz gut gewappnet ist. Zusammengefasst lässt sich sagen, dass die Lage ernst, aber nicht dramatisch ist. Bevor also 42 neue Straftatbestände geschaffen werden, empfiehlt es sich, einen Moment innezuhalten. Treten neue Phänomene auf, so droht aus einem Gefühl der Überforderung und des Aktionismus heraus gehandelt zu werden. Dies führt leider allzu häufig zu Umständen, wie sie eben beschrieben wurden: Straftatbestände, die unbestimmt sind; unbestimmte Tathandlungen, die sich überschneiden und bei denen niemand genau weiß, wo denn eigentlich die Strafbarkeit genau anfängt und wo sie aufhört. Stattdessen sollte zunächst konkret aufgearbeitet werden, was genau passiert – und erst dann präzise Umschreibungen für einen Straftatbestand geschaffen werden. Auch sollte Problemen hinsichtlich einer effektiven Strafverfolgung nicht mit Maßnahmen auf Ebene des materiellen Rechts begegnet werden, die allzu oft entweder keine oder nicht die erwünschten Wirkungen haben. Als Prämisse muss dabei immer gelten, dass das Strafrecht zurückhaltend einzusetzen ist: Es handelt sich um das empfindlichste Mittel, das dem Staat zur Verfügung steht. Deshalb muss es immer das *letzte* Mittel der Wahl sein, nicht das *erste*.

> Das Strafrecht ist das empfindlichste Mittel des Staates – es muss immer das *letzte* Mittel sein

[51] Dieses wird daher z.T. in den Tatbestand hineingedeutet, siehe etwa *Wieck-Noodt*, in: MüKo-StGB, Bd. 5, 3. Aufl. 2019, § 303a Rn. 9; vgl. auch *Hecker*, in: Schönke/Schröder-StGB, 30. Aufl. 2019, § 303a Rn. 3.

[52] Siehe beispielsweise *Zaczyk*, in: NK-StGB, 5. Aufl. 2017, § 303a Rn. 4: „Die in der Lit. vorgenommenen Konkretisierungen sind nicht Gesetzesauslegung, sondern Tatbestandsergänzungen; diese Aufgabe muss aber der Gesetzgeber leisten. Die Norm ist deshalb wegen Verstoßes gegen Art. 103 Abs. 2 GG verfassungswidrig."

Literatur

Biermann, Kai/ Middelhoff, Paul/ Sehl, Markus: Angriff auf die Herzkammer. Zeit Nr. 52/2020.

Bundeskriminalamt: Bundeslagebild Cybercrime 2020, abrufbar unter https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html.

Bundeskriminalamt: Bundeslagebild Cybercrime 2021, abrufbar unter https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html.

Bundeskriminalamt: Polizeiliche Kriminalstatistik 2019, Jahrbuch Band 1 Fälle – Aufklärung – Schaden, abrufbar unter https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2019/PKSJahrbuch/pksJahrbuch_node.html.

Bundeskriminalamt: Polizeiliche Kriminalstatistik 2020, abrufbar unter https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2020/pks2020_node.html;jsessionid=4A84B3425AA557AF83E90E710259F35B.live611.

Bundeskriminalamt: Polizeiliche Kriminalstatistik 2021, abrufbar unter https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2021/pks2021_node.html;jsessionid=4A84B3425AA557AF83E90E710259F35B.live611.

Buermeyer, Ulf: Warum der Vorschlag zur Strafbarkeit der „Datenhehlerei“ die Pressefreiheit gefährdet (Update), 17.5.2015, abrufbar unter https://netzpolitik.org/2015/warum-der-vorschlag-zur-strafbarkeit-der-datenhehlerei-die-pressefreiheit-gefaehrdet/.

Dreißigacker, Arne/ Fahl, Sascha/ Huaman, Nicolas/ von Skarczinski, Bennet/ Stransky, Christian/ Wollinger, Gina Rosa: Cyberangriffe gegen Unternehmen. Projektabschlussbericht, Kriminologisches Forschungsinstitut Niedersachsen e.V. (KFN), Hannover, September 2021, abrufbar unter https://kfn.de/publikationen/kfn-forschungsberichte/.

Flade, Florian/Tanriverdi, Hakan: Hackerjagd mit Hindernissen, 22.04.2021, abrufbar unter https://www.tagesschau.de/investigativ/br-recherche/hackerjagd-101.html.

Herfurth, Constantin /Drews, Daniel: Verfassungsbeschwerde gegen Straftatbestand der Datenhehlerei (§ 202d StGB), Newsdienst ZD-Aktuell 2017, 05490.

Joecks, Wolfgang/ Miebach, Klaus (Hg.): Münchener Kommentar zum Strafgesetzbuch, Band 5, 3. Auflage, München 2019.

Kindhäuser, Urs/ Neumann, Ulfried/Paeffgen, Hans-Ulrich (Hg.): Strafgesetzbuch. 5. Auflage, Baden-Baden 2017.

Klaas, Arne: „White Hat Hacking" – Aufdecken von Sicherheitsschwachstellen in IT-Strukturen. Grenzen der Strafbarkeit von ethischen Hacking-Angriffen. Multimedia und Recht 2022, S. 187-192.

Netzpolitik.org: Digitaler Angriff auf den Bundestag: Investigativer Bericht zum Hack der IT-Infrastruktur der Linksfraktion, 19.06.2015, abrufbar unter https://netzpolitik.org/2015/digitaler-angriff-auf-den-bundestag-investigativer-bericht-zum-hack-der-it-infrastruktur-der-linksfraktion/.

Neubacher, Frank: Kriminologie. 4. Auflage, Baden-Baden 2020.

Rengier, Rudolf: Strafrecht Allgemeiner Teil, 13. Auflage, München 2021.

Ders.: Strafrecht Besonderer Teil I. Vermögensdelikte, 24. Auflage, München 2022.

Ders.: Strafrecht Besonderer Teil II. Delikte gegen die Person und die Allgemeinheit, 23. Auflage, München 2022.

Scherschel, Fabian A.: AKW Grundremmingen: Infektion mir Uralt-Schadsoftware, 22.04.2016, abrufbar unter https://www.heise.de/security/meldung/AKW-Gundremmingen-Infektion-mit-Uralt-Schadsoftware-3188599.html.

Schönke/Schröder, Strafgesetzbuch. Kommentar, 30. Auflage, München 2019.

Singelnstein, Tobias/ Kunz, Karl-Ludwig: Kriminologie. Eine Grundlegung. 8. Auflage, Bern 2021.

Spiegel.de: MediaMarkt und Saturn offenbar von Ransomware betroffen, 08.11.2021, abrufbar unter https://www.spiegel.de/netzwelt/gadgets/mediamarkt-und-saturn-offenbar-von-ransomware-betroffen-a-22695fa6-145a-4470-b774-6de0c61290e8.

Spiegel.de: Spur der Uniklinik-Hacker soll nach Russland führen, 22.09.2020, abrufbar unter https://www.spiegel.de/netzwelt/web/duesseldorf-spur-der-uni-klinik-hacker-soll-nach-russland-fuehren-a-a0430786-251e-4cba-af9c-a7599f14f5e8.

Statistisches Bundesamt: Fachserie 10 Reihe 3, 2020, abrufbar unter https://www.destatis.de/DE/Service/Bibliothek/_publikationen-fachserienliste-10.html.

SüddeutscheZeitung.de: Ein Jahr nach Hacker-Angriff auf Uniklinik: Keine Spur, 03.09.2021, abrufbar unter https://www.sueddeutsche.de/panorama/kriminalitaet-duesseldorf-ein-jahr-nach-hacker-angriff-auf-uniklinik-keine-spur-dpa.urn-newsml-dpa-com-20090101-210903-99-74876.

Universitätsklinikum Düsseldorf: IT-Ausfall an der Uniklinik Düsseldorf, 17.09.2020, abrufbar unter https://www.uniklinik-duesseldorf.de/ueber-uns/pressemitteilungen/detail/it-ausfall-an-der-uniklinik-duesseldorf.

v. Heintschel-Heinegg, Bernd (Hg.): Beck'scher Onlinekommentar StGB. 53. Edition, Stand: 01.05.2022, München 2022.

Wessels, Johannes/Beulke, Werner/Satzger, Helmut: Strafrecht Allgemeiner Teil, 51. Auflage, Heidelberg 2021.

Wessels, Johannes/Hettinger, Michael/Engländer, Armin: Strafrecht Besonderer Teil 1. Straftaten gegen Persönlichkeits- und Gemeinschaftswerte, 45. Auflage, Heidelberg 2021.

Wessels, Johannes/Hillenkamp, Thomas/Schuhr, Jan: Strafrecht – Besonderer Teil 2. Straftaten gegen Vermögenswerte, 44. Auflage, Heidelberg 2021.

IMPRESSIONEN AUS DER DISKUSSION...

„Stellt sich bei dem Fall der Uniklinik mit Blick auf den Tod der Patientin eigentlich noch ein Problem in der objektiven Zurechnung oder der Kausalität?“

„Die Kausalität wäre kein Problem gewesen, sofern man hätte nachweisen können, dass das Opfer überlebt hätte, wenn es früher behandelt worden wäre. Die objektive Zurechnung wäre dann – sofern man den Irrtum mal außen vor lässt – an und für sich auch kein Problem. Woran könnte man da denken? Zunächst an einen atypischen Kausalverlauf – doch ist es in einem Krankenhaus nicht so abwegig, dass man die Notaufnahme schließen muss, wenn alle Systeme nicht mehr funktionieren und man auf wesentliche Informationen nicht mehr zugreifen kann. Und so etwas wie ein eigenverantwortliches Dazwischentreten Dritter, das die Zurechnung unterbricht, käme eigentlich auch nicht in Betracht. Natürlich war da irgendein Mensch, der entschieden hat, die Krankenwagen statt nach Düsseldorf nach Wuppertal zu schicken. Aber diese Entscheidung wurde nur getroffen, um die Ausgangsgefahr, die von den Täterinnen oder Tätern geschaffen wurde, zu verringern. Dann handelt es sich aber nicht um ein eigenverantwortliches Dazwischentreten, das die Zurechnung unterbricht, weil immer noch die Ausgangsgefahr – die durch die Verschlüsselung geschaffen wurde – in dem Erfolg fortwirkt. Das heißt, die wertende Betrachtung der objektiven Zurechnung – die Frage danach: wem ist der Erfolg als Werk zuzurechnen? – würde zu dem Ergebnis kommen, dass dies die Personen sind, die das System verschlüsselt haben, weil sie damit die Ausgangsgefahr geschaffen haben, die in dem Tod noch fortwirkt.“

„Was ist eigentlich mit Cybermobbing? Das ist leider noch nicht flächendeckend vom Strafrecht geregelt – aber sicher auch schwierig zu definieren."

„Cybermobbing ist kein Rechtsbegriff, das macht es in der Tat etwas schwierig. Cybermobbing kann ja ganz vieles sein: Wenn beispielsweise jemand beleidigt wird, ist das im Rahmen der Beleidigungsdelikte eigentlich durchaus flächendeckend abgedeckt – so flächendeckend, wie Beleidigungen eben generell abgedeckt sind. Das heißt, ob ich jetzt jemanden im Real Life beleidige oder im Internet, macht für die Strafbarkeit erst einmal keinen Unterschied. Wobei das nicht ganz stimmt: Es wird sogar zum Teil *härter* bestraft, wenn es im Internet passiert. Wenn man einen Blick auf die Beleidigungsdelikte in §§ 185 ff. StGB wirft, sieht man, dass da in der letzten Zeit an vielen Stellen nachgeschärft wurde, um Taten im digitalen Raum entsprechend zu bestrafen. Auch Bedrohungen gemäß § 241 StGB können unter den Begriff Cybermobbing gefasst werden – selbstverständlich ändert sich auch hier an der Strafbarkeit nichts, wenn man eine Bedrohung auf digitalem Wege übermittelt. Gleiches gilt für das Nachstellen in § 238 StGB: Wenn ich jemanden stalke, macht es keinen Unterschied, ob ich mich vor die Haustür der Person stelle oder digitale Wege suche, um die Person zu belästigen. Es lässt sich also nicht pauschal sagen, dass Cybermobbing unzureichend kriminalisiert ist – es gilt immer genau zu schauen, welches konkrete Verhalten im Raum steht."

„In welchem Maße wird bei solchen Delikten üblicherweise, wenn überhaupt, verurteilt?"

„Das Strafmaß der hier einschlägigen Delikte ist ja relativ weit gefasst und reicht von Geldstrafen bis zu mehreren Jahren Haft. Da existieren keine fixierten Richtmaße, wie dieses Strafmaß im konkreten Fall ausfällt, sondern das obliegt der abwägenden Einzelfallentscheidung des Gerichts. In einem Fall wie dem der Uniklinik liegen natürlich ganz gravierende Folgen vor: Da war eine große Klinik mit sehr vielen Patientinnen und Patienten betroffen, deren Betrieb infolge der Verschlüsselung komplett heruntergefahren werden musste. Diese konkreten Folgen müssten natürlich bei der Strafzumessung berücksichtigt werden. Wie das dann im Einzelfall aussieht, ist aber schwer zu prognostizieren. Das Strafrecht ist an vielen Stellen schon sehr konkret, doch diese Konkretheit reicht eigentlich immer nur bis zum Schuldspruch – also bis zu dem Punkt, an dem man sagt: Strafe ja oder nein."

MISSBRAUCHS-DARSTELLUNGEN UND SEXUELLER MISSBRAUCH IM NETZ

THOMAS GOGER*

Thomas Goger ist seit der Einrichtung der Zentralstelle Cybercrime Bayern bei der Generalstaatsanwaltschaft Bamberg im Jahr 2012 deren stellvertretender Leiter. Seit dem 1. Oktober 2020 leitet er dort das Zentrum zur Bekämpfung von Kinderpornografie und sexuellem Missbrauch im Internet.

* Der Hanns-Seidel-Stiftung ist an dieser Stelle für die Genehmigung zum Wiederabdruck des Textes zu danken, siehe: *Goger, Thomas*: Missbrauchsdarstellungen und sexueller Missbrauch im Netz. Ein Blick aus der Praxis der Ermittlungsbehörden, in: Schmid, Sarah/ Schmid, Susanne (Hg.): Kinderschutz stärken. Prävention und Bekämpfung von sexuellem Kindesmissbrauch, Aktuelle Analysen Nr. 88, München 2021, S. 146 – 153.

Seit dem 1. Oktober 2020 ermitteln in Bamberg die Staatsanwältinnen und Staatsanwälte des Zentrums zur Bekämpfung von Kinderpornografie und sexuellem Missbrauch im Internet in besonders schwerwiegenden oder komplizierten Verfahren. In dieser Zeit konnten bereits mehrere beachtliche Erfolge erzielt werden. Die Erfahrung zeigt aber auch: Ermittlungen wegen Kinderpornografie gehen leider nie wirklich zu Ende.

I. Einleitung

Eine Reihe von die Öffentlichkeit aufrüttelnden Fällen der organisierten Verbreitung von Kinderpornografie und des schweren sexuellen Missbrauchs von Kindern haben dazu geführt, dass dieser Deliktsbereich in den letzten Jahren noch stärker in den Fokus von Politik und Strafverfolgungsbehörden gerückt ist. Es ist nun allen klargeworden, was sich aus Statistiken, Lagebildern und den Berichten von Ermittlern und Staatsanwälten schon lange ergibt: Die Omnipräsenz elektronischer Kommunikationsmittel, der Always-On-Status von Endgeräten aller Art, die ständige Verfügbarkeit digitaler Aufnahme- und Abspielgeräte treiben die Fallzahlen von Jahr zu Jahr in neue Höhen. Dabei ist für jeden, der sich mit dieser Art von Kriminalität befasst, offensichtlich: Wir befinden uns bei der Ausleuchtung des Dunkelfeldes immer noch am Anfang.

Die Fallzahlen von Kinderpornografie im Netz steigen kontinuierlich an

Zwei Trends machen zudem besonders Sorgen: Nach überzeugenden Berichten derer, die sich bereits über Jahre und Jahrzehnte mit kinderpornografischem Material befassen müssen, ist eine Tendenz zu immer härterem Material erkennbar. Auch die „Verfügbarkeit" von Kindern für die Täter wird durch die modernen Kommunikationsmittel leichter. Das Internet ermöglicht es einem Täter in Hamburg ohne weiteres, einen Mittäter in Wien zu finden, der bereit ist, sein eigenes Kind am nächsten Wochenende für Missbrauchstaten zur Verfügung zu stellen. Über Online-Dienste können Missbrauchstaten gar am anderen Ende der Welt bestellt, live per Videostreaming verfolgt und aktiv beeinflusst werden.

Moderne Kommunikationsmittel machen Kinder für die Täter „verfügbarer"

II. Die Täterinnen und Täter

Bei der Zentralstelle Cybercrime Bayern (ZCB) wurde zum 1. Oktober 2020 vom Bayerischen Staatsminister der Justiz, Georg Eisenreich, das Zentrum zur Bekämpfung von Kinderpornografie und sexuellem Missbrauch im Internet (ZKI) geschaffen. Verbunden mit der Einrichtung dieser Spezialeinheit war eine deutliche Ausweitung der personellen Ressour-

cen. Bereits seit ihrer Gründung Anfang 2015 spielt der Kampf gegen sexuelle Kindesausbeutung im Netz in der Arbeit der ZCB eine wesentliche Rolle.

Dabei wurde schnell deutlich, dass eine große Bandbreite an Täterprofilen zu verzeichnen ist und dass letztlich alle Bereiche der Gesellschaft betroffen sind: Die Staatsanwältinnen und Staatsanwälte haben es mit Teenagern zu tun, die Bilder und Videos von sich zum Austausch mit dem Partner hergestellt haben, ohne sich der Strafbarkeit bewusst zu sein, mit „Gelegenheitstätern", auf deren Festplatten sich neben Kinderpornografie meist auch riesige Bestände nicht pönalisierter Pornografie finden, mit WhatsApp-Gruppen, in denen kinderpornografisches Material neben anderen inkriminierten Medien zur vermeintlichen Belustigung viral verbreitet wird, aber auch mit Tätern, die eine gefestigte pädophile Prägung aufweisen, sich in hermetisch abgeschotteten Zirkeln bewegen und die ohne weiteres bereit und in der Lage sind, den Schritt vom Konsum kinderpornografischer Inhalte zum tatsächlichen Missbrauch zu gehen.

Die MiKADO-Studie der Universität Regensburg gelangte 2015 zu der Feststellung, dass die Prävalenz sexueller Fantasien mit Kindern in der männlichen deutschen Bevölkerung bei 4,4 % liegt. Die Prävalenz sexueller Missbrauchserfahrungen bei jungen Erwachsenen lag bei 8,5 %. In der forensischen Praxis spielen nahezu ausschließlich männliche Beschuldigte eine Rolle. Anklagen gegen Täterinnen sind die absolute Ausnahme.

Berücksichtigt man, dass in der wissenschaftlichen Literatur teilweise von einem nicht unerheblichen Anteil weiblicher Täterinnen ausgegangen wird,[1] stellt sich die Frage, ob hier ein blinder Fleck der Ermittlungsbehörden vorliegt, und wenn ja, wie auch bei den Täterinnen das Dunkelfeld weiter aufgehellt werden kann.

Die Altersspanne der Täter reicht von strafunmündigen Kindern bis in das hohe Rentenalter. Auch bei Beruf und sozialem Status spiegelt sich in den Ermittlungsakten regelmäßig die Zusammensetzung der Gesellschaft wider, zuletzt beim koordinierten Vollzug von 50 Durchsuchungs- und Beschlagnahmebeschlüssen in ganz Bayern im Rahmen der Operation Weckruf 2022, deren Ergebnisse am 26. Januar 2022 von ZKI und Bayerischem Landeskriminalamt (BLKA) im Beisein der Staatsminister Eisenreich und Herrmann in München vorgestellt wurden.[2] Auch hier fand sich bei den Tatverdächtigen eine ganze Palette von Berufen und Tätigkeiten.

---

1 Die MiKADO-Studie zum Beispiel berichtet von einem Täterinnenanteil von 20 % bei den erfassten Fällen sexuellen Kindesmissbrauchs.

2 Siehe die Pressemitteilung des Bayerischen Staatsministeriums der Justiz.

III. Die Taten

Die Operation Weckruf 2022, die sich gegen 55 Beschuldigte im Alter zwischen 18 bis 73 Jahren richtete, als bislang bayernweit größte Durchsuchungsaktion gegen Kinderpornografie und Cyber-Grooming hat zudem deutlich gemacht, wie unterschiedlich die Quellen und Kanäle für das in der Szene zirkulierende kinderpornografische Material sind: Ein Großteil der Verfahren hatte seinen Ursprung in Meldungen der Internetwirtschaft über das National Center for Missing & Exploited Children (NCMEC). Andere Verfahren nahmen ihren Anfang im vom ZKI gemeinsam mit mehreren bayerischen Polizeidienststellen erfolgreich betriebenen Monitoring von Filesharing-Diensten. Wiederum weitere Verfahren wurden vom ZKI nach Hinweisen ausländischer oder nationaler Partnerdienststellen eingeleitet. Diese Vielfalt schlägt sich auch in einer Vielgesichtigkeit der vor Gericht verhandelten Fälle nieder, was einige Beispiele aus der erfolgreichen Arbeit des ZKI der vergangenen Monate verdeutlichen sollen:

Ermittlungsverfahren wegen Kinderpornografie sind ausgesprochen heterogen

Im November 2020 wurde ein bereits mehrfach einschlägig vorbestrafter Angeklagter durch das Landgericht Augsburg u.a. wegen schweren sexuellen Missbrauchs von Kindern zu einer Gesamtfreiheitsstrafe von über vier Jahren verurteilt. Dem ZKI gelang in aufwändigen Ermittlungen der Nachweis, dass sich der Mann an dem zum Tatzeitpunkt fünf- bis siebenjährigen Sohn eines befreundeten Ehepaars sexuell vergangen hatte.

Das Jugendschöffengericht des Amtsgerichts Amberg verurteilte im Januar 2021 einen zu den Tatzeitpunkten teilweise noch jugendlichen Angeklagten aus dem Landkreis Schwandorf, der als Moderator mehrerer Kinderpornografie-Plattformen im Darknet fungierte, zu einer Jugendstrafe von zwei Jahren und neun Monaten.

In einem beim ZKI zunächst wegen des Tatverdachts der Verbreitung kinderpornografischer Schriften geführten Verfahren konnte nachgewiesen werden, dass der Angeklagte über den Internetdienst Skype mehrfach Live-Video-Chats geführt hatte, in denen Kinder im Ausland auf seine Veranlassung und nach seinen Anweisungen schwer sexuell misshandelt und vergewaltigt worden waren. Er wurde vom Landgericht München I im April 2021 zu einer Gesamtfreiheitsstrafe von sechs Jahren verurteilt.

IV. Ermittlungen ohne Ende

Die forensische Arbeit von ZCB und ZKI hat in den vergangenen Jahren mehr als einmal bewiesen, dass Ermittlungen wegen Kinderpornografie und sexuellen Missbrauchs im Internet leider nie wirklich zu Ende sind. Es finden sich regelmäßig im Rahmen der Auswertung von sichergestellten Datenträgern, Computern und Smartphones Hinweise, die Ansätze zur Ermittlung weiterer Täter und – mindestens genauso wichtig – zur Identifizierung von Opfern liefern können. Sei es, dass Kommunikationspartner des Beschuldigten aufgedeckt werden können, sei es, dass sich bislang unbekanntes kinderpornografisches Material findet, welches dann besonders sorgfältig auszuwerten ist.

Entscheidend für den Ermittlungserfolg sind Fachkunde und Akribie

Wie wichtig ein fachkundiges und akribisches Arbeiten der Ermittlungsbehörden hierbei ist, beweist der Fall eines Würzburger Logopäden, der – nach Anklage durch die ZCB – vom Landgericht Würzburg im Mai 2020 wegen mehrerer Fälle des schweren sexuellen Missbrauchs von ihm zur Behandlung anvertrauten Jungen zu einer Gesamtfreiheitsstrafe von über 11 Jahren verurteilt wurde.[3] Bereits unmittelbar nach der Festnahme des Mannes im März 2019 wurde – parallel zu den gegen ihn geführten Ermittlungen – alles darangesetzt, das beschlagnahmte Material gewissenhaft auch auf weitere Ermittlungsansätze zu überprüfen. Die Erfolge dieser vor allem vom Bayerischen Landeskriminalamt geschulterten Bemühungen können sich sehen lassen: Knapp 50 weitere Täter konnten aus der Anonymität des Darknets geholt und identifiziert werden. Neben rund 30 in Deutschland wohnenden Beschuldigten waren weitere Personen im Ausland aufhältig, so dass die entsprechenden Ermittlungsverfahren nach Belgien, Frankreich, Italien, Österreich und in die Schweiz abgegeben wurden.

Spuren führen oft ins Ausland, aber auch wieder zurück nach Deutschland

Bei zahlreichen weiteren Nutzern von kinderpornografischen Darknet-Plattformen konnten vielversprechende Hinweise und Spuren zu deren Identifizierung gewonnen werden, die an Strafverfolgungsbehörden in Deutschland, Albanien, Dänemark, Ecuador, England, Jordanien, Mexiko, Polen, Russland, Tschechien und in den USA übermittelt wurden und die dort zur Grundlage weiterer Ermittlungen gemacht werden konnten. Es ist nicht auszuschließen, vielmehr sogar zu erwarten, dass die nun aufgrund dieser Hinweise im Ausland geführten Ermittlungen ihrerseits in der Zukunft zu neuen Ablegern führen werden, die zurück nach Deutschland weisen.

So befriedigend es also ist, einen Täter überführen und vielleicht sogar ein Kind aus einer Missbrauchssituation befreien zu können, Staatsanwälte,

IT-Forensiker und Polizeibeamte können sich nie auf dem Erreichten ausruhen. Der nächste Täter und das nächste Opfer sind oft nur eine digitale Spur weit entfernt.

V. Herausforderungen für die Ermittlungsbehörden

Auch wenn im Kampf gegen Kinderpornografie und sexuellen Missbrauch im Internet von den Staatsanwälten des ZKI tagtäglich Erfolge erzielt werden, stehen sie doch an vielen Stellen auch vor kaum zu überwindenden Herausforderungen. Zu nennen ist an erster Stelle die in Deutschland seit Jahren gänzlich fehlende Verkehrsdatenspeicherung.

Aufgrund dessen, dass IP-Adressen meist dynamisch von den Providern vergeben und durch technische Maßnahmen dieselbe IP-Adresse unter Umständen auch einer Vielzahl von Kunden gleichzeitig zugewiesen werden kann, hat diese rechtliche Leerstelle zur Folge, dass es in vielen Fällen nicht mehr möglich ist, eine IP-Adresse, die zum Beispiel aus dem Ausland übermittelt wurde und die im Zusammenhang mit der Verbreitung kinderpornografischer Inhalte aufgefallen ist, noch einem konkreten Anschlussinhaber zuzuordnen. Dies wiederum führt dazu, dass Ermittlungsverfahren oftmals schon am Ende sind, bevor sie überhaupt richtig beginnen konnten. Der Europäische Gerichtshof hat deutlich gemacht, dass schon aktuell durchaus Spielräume für eine Bevorratung dieser für erfolgreiche Ermittlungen so wichtigen Daten bestehen. Es wäre nun am Gesetzgeber, diese bedenkliche Strafverfolgungslücke endlich zu schließen.

Eine Abwägung der durch eine begrenzte Wiedereinführung der Vorratsdatenspeicherung tangierten Rechtsgüter sollte sich davon leiten lassen, dass der Kinderschutz sicherlich keinen geringeren Stellenwert hat als der Datenschutz. Die anhaltenden Initiativen des bayerischen Justizministers, diesen Missstand auf europäischer und auf Bundesebene zu beheben, genießen jedenfalls die volle Unterstützung der staatsanwaltschaftlichen Praxis.

VI. Fazit

Mit der Schaffung des ZKI hat die bayerische Justiz eine wichtige Strukturentscheidung getroffen, um im Kampf gegen sexuelle Kindesausbeutung im Netz noch schlagkräftiger agieren zu können. Bereits erzielte Er-

[3] Süddeutsche.de vom 25.5.2020.

mittlungserfolge beweisen, dass durch die Bündelung technischer und juristischer Sachkunde bei einer staatsanwaltschaftlichen Spezialeinheit viel erreicht werden kann. Die Jahr für Jahr ansteigenden Fallzahlen erinnern aber beständig daran, dass wir noch lange nicht am Ziel sind. Für die Staatsanwälte des ZKI bleibt jedenfalls viel zu tun: Sind in den vergangenen Jahren rund 1.000 Verfahren wegen Straftaten gegen die sexuelle Selbstbestimmung in Bamberg eingegangen, waren es 2021 bereits 3.236.

Steigende Fallzahlen beweisen: Wir sind noch lange nicht am Ziel.

Literatur

Abteilung für Forensische Psychiatrie und Psychotherapie der Universität Regensburg: Missbrauch von Kindern: Aetiologie, Dunkelfeld, Opfer (MIKADO), 2015, abrufbar unter http://www.mikado-studie.de/tl_files/mikado/upload/MiKADO_Zusammenfassung.pdf.

Bayerisches Staatsministerium der Justiz: Bayernweiter Aktionstag im Kampf gegen Kinderpornografie, 26.1.2022, abrufbar unter https://www.justiz.bayern.de/presse-und-medien/pressemitteilungen/archiv/2022/7.php.

Süddeutsche Zeitung: Logopäde missbraucht behinderten Jungen – lange Haftstrafe. Süddeutsche.de vom 25.5.2020, abrufbar unter https://www.sueddeutsche.de/bayern/wuerzburg-logopaede-sexueller-missbrauch-urteil-1.4917091.

DIGITALE GEWALT – MÖGLICHKEITEN UND HERAUSFORDERUNGEN BEI IHRER BEKÄMP-FUNG

JOSEPHINE BALLON, HATEAID

Josephine Ballon ist Sprecherin der Beratungsstelle HateAid gGmbH. HateAid bietet Beratungen und Prozesskostenhilfe für Betroffene von digitalen Beleidigungen und Hassnachrichten an. Die gemeinnützige GmbH vertrat etwa Renate Künast (MdB) und die Klimaaktivistin Luisa Neubauer.

Digitale Gewalt betrifft uns alle. Sie wird als politisches Mittel gezielt genutzt, um gerade Menschen, die sich politisch, aktivistisch oder journalistisch engagieren, zu diskreditieren und den öffentlichen Diskurs zu manipulieren. Umso wichtiger sind ein effektiver Zugang zum Recht sowie staatliche Institutionen, die den Betroffenen zur Seite stehen. Daran fehlt es leider zu oft. HateAid unterstützt die Menschen dabei, ihre Rechte effektiv durchzusetzen und zeigt auf, was wir alle tun können, um uns vor digitaler Gewalt zu schützen oder uns im Ernstfall rechtlich dagegen zu wehren.

HateAid unterstützt Menschen dabei, ihre Rechte effektiv durchzusetzen

I. Wer sind wir

HateAid ist die erste Beratungsstelle allein für Betroffene von digitaler Gewalt in ganz Deutschland. Wir bieten in erster Linie Betroffenenberatung an, die eine emotional-stabilisierende Erstberatung sowie Sicherheits- und Kommunikationsberatungen umfasst. Auch Rechtsdurchsetzung ist uns ein besonderes Anliegen. Diese verfolgen wir im Rahmen unserer Prozesskostenfinanzierung, mit der wir es Betroffenen digitaler Gewalt ermöglichen sich ohne eigenes Kostenrisiko auch juristisch zur Wehr zu setzen. Wir unterstützen Betroffene unter anderem bei der Beweissicherung sowie finanziell bei der Erstattung von Strafanzeigen und Zivilklagen.

Darüber hinaus ist es uns ein besonderes Anliegen, die Rahmenbedingungen insgesamt zu verbessern. Hierfür arbeiten wir mit den Strafverfolgungsbehörden und der Justiz zusammen und sensibilisieren sie für die Bedürfnisse der Betroffenen. In der Politik setzen wir uns dafür ein, dass sich die Rechte der Betroffenen auch in der nationalen und europäischen Gesetzgebung widerspiegeln.

II. Was passiert im Netz?

Hass im Netz ist heutzutage allgegenwärtig. Aus Umfragen wissen wir, dass bereits mehr als 60 % der Internetnutzenden schon einmal Hass im Netz gesehen haben. Noch gravierender ist das Bild bei den jungen Erwachsenen zwischen 18 und 35. Hier geben auf europäischer Ebene 91 % an, bereits mehrmals Zeug*innen von digitaler Gewalt geworden zu sein. 50 % waren sogar schon einmal selbst betroffen.[1] Das zeigt, dass es vor allem die jungen Erwachsenen sind, die massiv von digitaler

Mehr als 60 % der Internetnutzenden haben schon einmal Hass im Netz gesehen

[1] HateAid, Grenzenloser Hass im Internet – Dramatische Lage in ganz Europa.

Gewalt betroffen sind. Das ist das Internet, mit dem junge Menschen heutzutage aufwachsen, die kein „vorher" und kein „nachher" kennen. Viele haben sich bereits an diese Situation gewöhnt. Das ist ein entscheidender Punkt. Denn an vielen Stellen messen wir mit zweierlei Maß: Was wir im Internet normal finden, weicht häufig von dem ab, was wir in der analogen Welt tolerieren würden.

1. Hass als Strategie

Es mag den Anschein erwecken, als wären alle Menschen in Deutschland extrem hasserfüllt und würden ihrer Wut im Internet freien Lauf lassen. Das ist allerdings nicht so. Wir wissen aus verschiedenen Studien, dass nur einige Wenige den Hass verbreiten. Diese Wenigen wissen die Besonderheiten des Internets auszunutzen. Eine Erhebung aus dem Jahr 2018 hat gezeigt, dass in den hasserfüllten Kommentarspalten von Facebook nur etwa 5% der User*innen für insgesamt 50 % der Likes verantwortlich sind.[2] Das zeigt sehr anschaulich, dass wir es mit organisierten Gruppen zu tun haben.

2. Hass als politisches Mittel

Der Hass ist dabei auch ein politisches Mittel, mit dem bestimmte Gruppierungen vor allem aus dem rechten und rechtsextremen Spektrum den Eindruck erwecken wollen, in der Mehrheit zu sein. Laut Statistik des Bundeskriminalamts zur politisch motivierten Kriminalität wurden im Jahr 2019 73 % der politisch motivierten Hasspostings dem rechten und rechtsextremen Bereich zugerechnet.[3] Rechtsextreme teilen untereinander sogar eigene Leitfäden, in denen steht, man solle anstelle von nur einem mehrere Accounts unterhalten, um ganz besonders effektiv vorgehen zu können. Weiterhin wird dazu geraten, keine strafrechtlich relevanten Aussagen zu tätigen, sondern stattdessen die Gegner*innen zu provozieren und sie durch die Plattform sperren zu lassen. Und trotzdem wird explizit gesagt: Beleidigen ist erlaubt. Gerade die Familie wird dabei als schwacher Punkt identifiziert. Das verdeutlicht, dass die Beleidigung gar nicht mehr als richtige Straftat wahrgenommen wird. Das gilt übrigens nicht nur für die Täter*innen, sondern auch für die Betroffenen. Auch sie haben sich schon so sehr daran gewöhnt, dass sie selbst drastische Beleidigungen nicht für strafbar halten. Vor allem persönliche Informationen werden missbraucht, um gezielt einzuschüchtern.

---

2 *Kreißel/Ebner/Urban/Guhl*, Hass auf Knopfdruck – Rechtsextreme Trollfabriken und das Ökosystem koordinierter Hasskampagnen im Netz, S. 12.

3 Bundeskriminalamt, Politisch motivierte Kriminalität im Jahr 2019 – Bundesweite Fallzahlen, S. 7.

3. Hass verschiebt den öffentlichen Diskurs

All das wirkt sich nicht nur auf die Betroffenen selbst aus. Vielmehr sind es wir alle, die hierdurch beeinflusst werden. 54 % der Internetnutzenden in Deutschland trauen sich bereits nicht mehr, ihre politische Meinung im Netz zu sagen.[4] Dieser Zustand sollte uns alle alarmieren, denn er führt dazu, dass sich mehr und mehr Menschen aus dem öffentlichen Diskurs im Internet zurückziehen. Dazu gehören vor allem Menschen, die marginalisierten Gruppen angehören, die sich aktivistisch, journalistisch oder kommunalpolitisch engagieren und deren Meinung auf diese Weise in der öffentlichen Debatte nicht mehr stattfindet. Das betrifft ganz besonders Frauen, die nicht nur die größte, sondern eine der am stärksten von digitaler Gewalt betroffene Gruppe sind und sich auch ganz spezifischen Angriffen ausgesetzt sehen. So wird der Diskurs einseitig zugunsten einer lauten Minderheit verschoben und der Meinungspluralismus im Internet grundlegend gefährdet.

> 54 % der Internetnutzenden in Deutschland trauen sich bereits nicht mehr, ihre politische Meinung im Netz zu sagen – besonders betroffen sind Frauen

II. Woran scheitern Betroffene?

Trotz der enormen gesellschaftlichen Relevanz digitaler Gewalt werden die Betroffenen leider zu oft alleingelassen. Es mangelt an Anlaufstellen, zu wenige Straftaten werden verfolgt und insgesamt werden den Betroffenen zu viele Hürden in den Weg gestellt.

1. Kaum Anlaufstellen

Betroffene finden kaum spezialisierte Anlaufstellen, die ihnen auf den digitalen Raum zugeschnittene Hilfe anbieten. Traditionelle Beratungsstellen, Frauenberatungsstellen oder solche im Bereich der Antirassismusarbeit sind oftmals mit Sachverhalten aus dem digitalen Raum überfordert.

> Betroffene finden kaum spezialisierte Anlaufstellen

2. Zu wenig Strafverfolgung

Daneben erleben wir nach wie vor grundlegende Defizite bei der Strafverfolgung von Hasskriminalität in Internet. Zu begrüßen ist es hingegen, dass sich in immer mehr Bundesländern spezialisierte Abteilungen

[4] Institut für Demokratie und Zivilgesellschaft, #Hass im Netz: Der schleichende Angriff auf unsere Demokratie, S. 28.

und Dezernate für die Verfolgung von Hasskriminalität im Internet bei den Polizeien und Staatsanwaltschaften herausbilden.

a) Anonyme Täter*innen

Das grundlegende Problem, dass viele Täter*innen nicht identifiziert werden können, bleibt weiterhin ungelöst. Es ist extrem einfach, sich mit völlig erfundenen Daten Social-Media-Profile anzulegen. Weil die großen Plattformen im Ausland sitzen, kann nur sehr eingeschränkt auf sie bzw. Daten der Täter*innen zugegriffen werden. Es braucht Rechtshilfeersuchen, die entweder zu lange dauern oder nicht beantwortet werden. Den Ermittlungsbehörden bleibt daher nur eine sehr aufwändige Recherche nach Ermittlungsansätzen. Meist sind das online auffindbare Hinweise auf die Identität des*der Täter*in, zum Beispiel der Name, der Wohnort oder das Geburtsdatum, welche dann gegebenenfalls durch Registerabfragen zur Identifizierung führen. Wir kooperieren mit einer spezialisierten Staatsanwaltschaft in Frankfurt am Main – die Zentralstelle für Internetkriminalität Hessen – und kommen hier auf eine Identifizierungsquote von einem Drittel. Was nach wenig klingt, ist für uns schon ein großer Erfolg. Beruhigend ist auch das Wissen, dass alle Ermittlungsansätze hier tatsächlich ausgeschöpft werden. So konnte in einem unserer Fälle etwa die Identifizierung über eine Hundesteuermarke auf einem Foto erfolgen.

> Täter*innen können nicht identifiziert werden

b) Verfahrenseinstellungen bei Beleidigungsdelikten

Ein weiteres Problem ist, dass die Strafverfahren wegen Beleidigungsdelikten in den meisten Fällen eingestellt werden. Warum ist das so? Kurz gesagt: Weil es einfach ist. Das besondere öffentliche Interesse ist schnell abgelehnt und die Sache auf den Privatklageweg verwiesen, um das Verfahren vom Tisch zu bekommen. Das verkennt natürlich, dass die Beleidigungsdelikte längst nicht mehr den Status einer „bloßen" Privatsache haben, den das Gesetz ihnen zuspricht. Denn wenn ich in Berlin sitze und von einem anonymen „Troll" in Stuttgart auf Facebook vor den Augen meiner Familie, meiner Arbeitskolleg*innen und anderer Nutzer*innen sexualisiert beleidigt und bloßgestellt werde, dann scheint es fast schon absurd, wenn die Staatsanwaltschaft mir sagt, es sei meine Privatsache, mich darum zu kümmern, dass hier ermittelt wird. Manches wird auch mangels öffentlichen Interesses oder wegen Geringfügigkeit eingestellt. Solche Bescheide, in denen Wörter wie „Geringfügigkeit" und „kein öffentliches Interesse an der Strafverfolgung" stehen, sind für die Betroffenen ein Schlag ins Gesicht.

> Strafverfahren wegen Beleidigungsdelikten werden in den meisten Fällen eingestellt

c) Komplizierte Anzeigenstellung

Auch gibt es immer noch zu hohe Hürden bei der Anzeigenstellung. Wenn man im Netz beleidigt wird, dann handelt es sich meistens nicht um einen isolierten Fall, sondern um eine Vielzahl von Vorfällen, die sich innerhalb kürzester Zeit wiederholt ereignen. Den Betroffenen wird dann auch noch abverlangt, Beweise zu sichern, Strafanträge zu stellen und die Unterlagen dann ausgedruckt zur Polizeidienststelle zu bringen. Auch heute ist es in Deutschland noch immer nicht flächendeckend möglich, Strafanzeigen online zu stellen. Selbst in Berlin, der Bundeshauptstadt, kann man bei der Online-Anzeige noch keine Screenshots hochladen. Das ist ein Zustand, der betroffenenunfreundlich ist und zu weniger Strafanzeigen führt, was dem Ziel zuwiderläuft, mehr Straftaten im Netz zu verfolgen.

> Auch heute ist es in Deutschland nicht flächendeckend möglich, Strafanzeigen online zu stellen

d) Fehlende Sensibilisierung von Behörden und Justiz

Betroffene berichten uns auch im Jahr 2022 noch, dass sie bei der Anzeigeerstattung nicht ernst genommen werden, dass ihr Fall bagatellisiert wird und sie sogar „Victim Shaming“ erleben. Es ist für Betroffene – vor allem, wenn es sich um junge Menschen handelt, für die das Internet ein essentieller Bestandteil der Teilhabe am sozialen Leben ist – schlicht lebensfremd, wenn ihnen gesagt wird: Melden Sie sich doch einfach ab oder schalten Sie das Smartphone aus, dann haben Sie das Problem nicht. Oder wenn man sich zum Beispiel in eine Frau hineinversetzt, die sexualisiert beleidigt wurde und die sich dann auf der Polizeidienststelle anhören muss, dass sie sich über solche Kommentare gar nicht wundern brauche, wenn sie ein Urlaubsfoto in einem kurzen Rock hochlädt. Das ist für die Betroffenen nicht nur ein traumatisches Erlebnis, sondern führt auch dazu, dass sie in Zukunft keine Strafanzeige mehr erstatten werden. Dadurch verlieren die Menschen das Vertrauen in den Rechtsstaat. Das ist ein sehr bedenklicher Zustand, der tagtäglich in unserer Beratung sichtbar wird. Die Betroffenen glauben, dass im Internet andere Gesetze gelten, wir all das nicht ändern können und einfach so hinnehmen müssen. Wir mahnen bei den Staatsanwaltschaften immer wieder an, das Personal für Ermittlungen im Internet zu schulen. Allzu häufig wird uns entgegengebracht, dass sich ein solcher Aufwand nicht lohne, wenn nur drei Straftaten im Jahr angezeigt werden. Das ist ein Dilemma, das erst einmal aufgelöst werden muss.

e) Zeugenschutz

Auch der Zeugenschutz ist ein großes Thema. Zwar wurden die Vorschriften bereits nachgebessert, jedoch besteht weiterhin Nachholbedarf. Das ist notwendig, damit die Täter*innen nicht über eine Einsichtnahme in die Ermittlungsakten herausfinden können, wer ich bin und wo ich wohne. Diese Daten offenzulegen, hält viele Betroffene davon ab, Straftaten anzuzeigen. Die Polizei muss die bereits vorhandenen Zeugenschutzvorschriften der §§ 68 ff. StPO konsequenter anwenden. Es ist nicht nachvollziehbar, warum dies nicht bereits passiert.

Auch im Bereich Zeugenschutz besteht Nachholbedarf

2. Zivilrechtliche Rechtsdurchsetzung

Unter Zugang zum Recht verstehe ich vor allem zivilrechtliche Rechtsdurchsetzung. Wie bereits erwähnt, bietet HateAid Prozesskostenfinanzierung für Zivilverfahren an. Das ist notwendig, weil ansonsten niemand klagen würde.

a) Der „Fall Künast" – fatales Signal an Betroffene

Der von HateAid unterstützte „Fall Künast" vor dem Landgericht Berlin hat im Jahr 2019 ein fatales Signal an Betroffene ausgesendet. Dabei ging es um ein Zivilverfahren, mit dem von Facebook Auskünfte zu Accountinhaberdaten erlangt werden sollten, die Frau Künast – so dachten wir zumindest – im Netz beleidigt haben. Doch das Gericht war anderer Meinung. Ausdrücke wie „Drecks Fotze" oder „Pädophilen-Trulla" seien keine Beleidigungen; das sei sachliche Kritik und die Sachauseinandersetzung im politischen Meinungskampf sei hier ganz klar gegeben. Um eine reine Diffamierung handele es sich in keinem der Fälle.[5]

Der „Fall Künast" vor dem Landgericht Berlin hat ein fatales Signal an Betroffene ausgesendet

Das Urteil stieß auf scharfe Kritik, auch seitens der Fachpresse, und das Gericht korrigierte sich anschließend in Bezug auf sechs von 22 Äußerungen selbst.[6] Sechs weitere Äußerungen hob dann das Kammergericht Berlin auf.[7] Die übrigen Fälle liegen nun beim Bundesverfassungsgericht. Wir sind gespannt auf die Entscheidung und hoffen auf einige wichtige verfassungsgerichtliche Impulse im Umgang mit Hass im Netz.[8]

5 LG Berlin, Beschluss v. 9.9.2019 – 27 AR 17/19, MMR 2019, 754.
6 LG Berlin, Beschluss v. 21.1.2020 – 27 AR 17/19, MMR 2019, 754.
7 KG Berlin, Beschluss vom 11.3.2020 – 10 W 13/20, MMR 2020, 867.
8 BVerfG, Beschluss v. 19.12.2021 – 1 BvR 1073/20, NJW 2022, 680: Inzwischen hat das BVerfG die Beschlüsse des LG und KG Berlin aufgehoben. Es bemängelt, dass die Gerichte die Beleidigungen nicht richtig geprüft hätten. Die Entscheidun-

b) Teure und langwierige Verfahren

Das liegt in erster Linie daran, dass ein Gerichtsverfahren für die Betroffenen oftmals schlichtweg zu teuer ist. Die besonders hohen Streitwerte bei Persönlichkeitsrechtsverletzungen auf Social Media führen zu einem hohen Kostenrisiko hinsichtlich der Gerichts- und Anwaltskosten. Hinzu kommen Verfahrensdauern von über einem Jahr. Da erscheint es vielen Menschen unverhältnismäßig, überhaupt aktiv zu werden. Denn die Betroffenen hoffen, dass der Facebook-Post von heute am nächsten Tag schon keine Aufmerksamkeit mehr erfährt. Doch das Internet vergisst nicht. Es holt viele Betroffene auch nach langer Zeit wieder ein. Letztlich führen diese hohen Hürden dazu, dass Nutzende bestärkt durch ihre früheren Erfahrungen glauben: „Das ist jetzt halt auf Social Media so." Hinzu tritt, dass die Erfolgsaussichten bei Fällen von Persönlichkeitsrechtsverletzungen extrem schwer zu bestimmen sind. Die Abwägung zwischen Meinungsfreiheit und Persönlichkeitsrechten ist schwierig und eine zuverlässige Prognose oftmals unmöglich. Eine Erfolgsgarantie gibt es in den wenigsten Fällen.

Die hohen Prozesskosten stellen eine zusätzliche Hürde für Betroffene dar

c) Prozesskostenfinanzierung und das solidarische Prinzip

Die Prozesskostenfinanzierung von HateAid basiert auf dem sogenannten „solidarischen Prinzip". Grundidee dabei ist, dass wir das Kostenrisiko tragen und dafür von den Betroffenen die erhaltene Geldentschädigung erhalten. Die Geldentschädigung fließt dann in unseren Fonds ein, um weitere Verfahren zu finanzieren. Jedoch trägt sich das System bei weitem noch nicht von selbst. Denn Geldentschädigungen werden von den Gerichten viel zu selten zugesprochen oder die verklagten Bürger*innen können die Zahlung nicht leisten.

Das „solidarische Prinzip" von HateAid reduziert das Kostenrisiko für Betroffene

3. Hass im Netz und die Grundrechte

Im Jahr 2020 hat sich das Bundesverfassungsgericht schon einmal zu einem Fall, der im Internet spielte, geäußert. Dort hat es bereits ermutigende Worte gefunden, die uns auch in der Verfassungsbeschwerde von Frau Künast, die HateAid weiterhin unterstützt, bestärken. In drei Beschlüssen hat das Bundesverfassungsgericht deutlich gemacht, dass das politische Engagement sehr wohl abwägungsrelevant ist. Viele Zivilgerichte haben das in der Vergangenheit verkannt.

gen entsprächen nicht den verfassungsrechtlichen Vorgaben an die Abwägung zwischen der Meinungsfreiheit und den Persönlichkeitsrechten der Betroffenen. Insbesondere seien die Besonderheiten des Internets – wie die Reichweite von Posts oder die Tatsache, dass sie über eine lange Zeit online bleiben können – nicht berücksichtigt worden; HateAid, Pressemitteilung v. 2.2.2022.

Das Bundesverfassungsgericht hat in den drei Beschlüssen klar beschlossen, dass nicht jede Kritik mit politischem Kontext automatisch Machtkritik ist.[9] Ein typisches Totschlagargument der Fachgerichte, das damit eingeschränkt wird. Das Bundesverfassungsgericht hat sogar gesehen, dass politisches Engagement nur dann erwartet werden kann, wenn auch ein effektiver Schutz der Persönlichkeitsrechte der Politiker*innen gewährleistet werden kann. Denn nur, wenn wir diesen Schutz gewährleisten, können wir sicherstellen, dass es weiterhin Menschen gibt, die sich für unsere Demokratie stark machen und gesellschaftliche Verantwortung übernehmen. Unsere Demokratie ist darauf angewiesen, dass es Menschen gibt, die sich für diese Arbeit zur Verfügung stellen.

> Nicht jede Kritik mit politischem Kontext ist automatisch Machtkritik

Das Bundesverfassungsgericht hat erfreulicherweise auch klargestellt, dass die Besonderheiten im Netz sehr wohl abwägungsrelevant sind. So kann einem Facebook-Post als schriftliche Äußerung mehr Sorgfalt abverlangt werden als einer mündlichen Äußerung. Natürlich ist eine Beleidigung am Gartenzaun oder im Straßenverkehr etwas ganz anderes als der Tweet, der für immer im Internet verewigt ist. Für mich hebt das Bundesverfassungsgericht damit ganz eindeutig hervor, dass das Verständnis von Beleidigungsdelikten im Netz als Privatsache überholt ist.

III. Wie können sich Betroffene schützen?

Bisher ging es in diesem Beitrag viel um die Frage, wo Probleme liegen und wie die Zustände im Netz sind. Der folgende Teil soll darauf eingehen, wie sich Betroffene schützen können.

1. Die eigenen Daten schützen

Zunächst sollten wir überlegen, welche persönlichen Daten wir im Netz von uns preisgeben. Das beginnt damit, dass wird die Privatsphäre-Einstellungen unserer Social-Media-Profile überprüfen – auch bei alten Profilen, die wir vielleicht schon vergessen haben. Wichtige Punkte hierbei sind: Wer hat Zugriff auf meine Daten? Mit wem bin ich befreundet? Wen sollte ich vielleicht aus meinen Kontakten löschen? Informationen wie das exakte Geburtsdatum oder die Privatanschrift haben im Internet

[9] BVerfG, Beschlüsse v. 19.5.2020 - 1 BvR 2459/19, 1 BvR 2397/19, 1 BvR 1094/19 und 1 BvR 362/18.

nichts verloren – auch nicht auf Verzeichnis-Seiten wie „dasoertliche.de“. Für die Erstellung von Passwörtern empfiehlt sich die Nutzung eines Passwortmanagers, um den Zugang sicher und robust zu gestalten. Daneben ist auch ein Notfallplan sinnvoll für den Fall, dass man von digitaler Gewalt betroffen ist. Denn es ist gut, auf einen solchen Plan zurückgreifen und sich sagen zu können: „Als erstes setzte ich meine Passwörter zurück, um zu verhindern, dass jemand Zugriff erlangt, dann setzte ich alle meine Profile auf ‚privat‘, damit keiner mehr was von mir sehen kann, und dann orientiere ich mich erstmal und versuche herauszufinden, was hier eigentlich passiert ist.“ Damit kann man manchmal schon schlimmeren Schaden verhindern.

Ein Notfallplan ist sinnvoll

2. Auskunftssperre im Melderegister eintragen lassen

Eine Melderegistersperre kann insbesondere für ehrenamtlich oder politisch aktive Personen interessant sein

Gerade diejenigen, die auf Online-Plattformen politisch oder ehrenamtlich aktiv sein wollen, möchte ich auf die Melderegistersperre nach § 51 BMG aufmerksam machen. Ich rate Ihnen nachdrücklich dazu, eine solche bei der Meldehörde am Wohnsitz zu beantragen. Durch eine Gesetzesänderung wurde nun in die gesetzliche Regelung explizit der Schutz vor Bedrohungen, Beleidigungen und unbefugter Nachstellung wegen beruflicher und ehrenamtlicher Tätigkeit als Grund für eine Melderegistersperre aufgenommen. Da es meist persönliche Informationen sind, die im Netz gegen die Betroffenen verwendet werden, sollte die Veröffentlichung der privaten Anschrift unbedingt vermieden werden.

Wenn man Probleme hat, sich bei der Behörde diese Sperre bewilligen zu lassen, kann es zum Beispiel helfen, frühere Strafanzeigen und andere Dokumente vorzulegen, die eine potentielle Gefährdung belegen. Auch ein Begleitschreiben einer Beratungsstelle wie HateAid einzuholen, aus dem deutlich wird, dass aus fachlicher Erfahrung eine konkrete Gefahr für die Person besteht, kann helfen.

Für Privatpersonen ist es in Deutschland leider extrem einfach über eine Melderegisterauskunft an die Anschrift zu gelangen. Das kostet gerade einmal zehn Euro und erfordert lediglich die Angabe eines berechtigten Interesses. Als berechtigtes Interesse gilt etwa, eine Person verklagen zu wollen, weil sie einem Geld schuldet. Das können auch andere Gründe sein, die leider unzureichend hinterfragt werden, weil sie oft nur glaubhaft gemacht werden müssen.

IV. Wie können sich Betroffene wehren?

Wenn wir uns anschauen, wie sich Betroffene von digitaler Gewalt wehren können, ist die erste wichtige Erkenntnis, dass das Netz kein rechtsfreier Raum ist, auch wenn die Betroffenen es häufig anders empfinden. Man sollte digitale Gewalt nicht einfach so hinnehmen, sondern dafür sorgen, dass die Inhalte entfernt werden. Daneben ist eine Strafanzeige bei der Polizei wichtig. Denn nur so können die Täter*innen bestraft werden und der Fall in der Kriminalitätsstatistik auftauchen.

1. Beleidigende Kommentare löschen und melden

Beleidigungen sollten nicht unkommentiert hingenommen werden. Wer eigene Kanäle betreibt, kann selbst löschen und verbergen. Auf öffentlich Social-Media-Seiten sollten die Inhalte gemeldet werden, und zwar nach dem Netzwerkdurchsetzungsgesetz (NetzDG) und nicht nach den Allgemeinen Geschäftsbedingungen. Denn nur dann findet auch tatsächlich eine juristische Prüfung statt. Zwar geschieht das nicht immer, aber so besteht wenigstens die Chance, dass die Meldung in Transparenzberichte einfließt und somit Evidenz über die Anzahl der relevanten Meldungen schaffen kann.

> Nur durch eine Meldung findet auch tatsächlich eine juristische Prüfung statt

Schwieriger wird es bei kleinen Websites, auf denen Inhalte über die eigene Person veröffentlicht wurden. So sind kleinere Blogs in manchen Fällen im Ausland registriert. Auch lassen sich deren Betreiber*innen nur schwer ermitteln. In diesen Fällen hilft es häufig nur, den Suchmaschineneintrag löschen zu lassen, indem man einen Löschantrag bei Google stellt.

2. Strafanzeige stellen

Derzeit liegt es damit leider immer noch an den Betroffenen, Straftaten selbst zu melden und anzuzeigen. Ich verstehe, wenn Menschen, die täglich mit einer Flut digitaler Gewalt konfrontiert sind, vor dem Aufwand zurückschrecken. In diesen Fällen ist es nachvollziehbar, Strafanzeigen auf besonders schlimme Fälle zu beschränken. Aber grundsätzlich gilt immer, dass Strafanzeigen gestellt werden sollten.

Denn Strafverfolgung hat einen wichtigen Abschreckungseffekt, wenn sie denn richtig funktioniert. Leider müssen wir feststellen, dass es bei Hass im Netz weiterhin große Defizite gibt. Bei den Screenings von besonders häufig betroffenen Personen durch unsere Mitarbeiter*innen

> Die Strafverfolgung hat einen wichtigen Abschreckungseffekt

stellen wir regelmäßig fest, dass die größten „Entgleisungen“ von Profilen kommen, die mit Fake- und Mehrfachidentitäten arbeiten und sich deshalb in Sicherheit wiegen. Mehr Anzeigen steigern auch das Bewusstsein der Strafverfolgungsbehörden dafür, wo es Probleme gibt und dass es sich um ein gesamtgesellschaftliches Problem handelt. Diese sind auf uns alle angewiesen: Denn es gibt keine „Internetpolizei“, die das Internet täglich durchkämmt und nach Straftaten durchsucht. Wenn die Zivilgesellschaft nichts meldet, dann wird auch nichts verfolgt.

Natürlich helfen wir auch gerne bei Strafanzeigen. Die App „Meldehelden“ oder das Meldeformular auf unserer Webseite, die wir ins Leben gerufen haben, unterstützt dabei, sehr niedrigschwellig Inhalte zu melden. Es ist darauf zu achten, dass der Strafantrag, den man für Beleidigungsdelikte braucht, schriftlich, also mit handschriftlicher Unterschrift, eingereicht wird. Das ist eine große Hürde, wenn man bedenkt, dass manche Betroffene tagtäglich mit diesen Inhalten überhäuft werden, und dann relativ oft Papiere ausdrucken, unterschreiben und im Zweifel per Post verschicken müssen. Eine Strafanzeige ist grundsätzlich mehrere Jahre möglich, während beispielsweise der Strafantrag für Beleidigung innerhalb von drei Monaten gestellt werden muss.

> Es sollte nicht vergessen werden, den Strafantrag handschriftlich zu unterschreiben

3. Beweise sichern

Wer eine effektive Rechtsdurchsetzung erreichen will, muss auch Beweise sichern. Das ist für die meisten Betroffenen eine große Herausforderung. Zumal die Inhalte bereits durch die Plattformen gelöscht sein können, nachdem sie gemeldet worden sind. Deswegen sollte man sich zuallererst immer mit der Beweissicherung beschäftigen. Hier reicht ein einfacher Screenshot oft nicht aus. Es müssen so viele Details wie möglich erkennbar sein, was insbesondere den Kommentar und Inhalt, den Kontext, Datum und Uhrzeit umfasst. Auch die URL sollte gesichert werden.

> Eine umfassende Beweissicherung hilft beim späteren Prozess

Um diese durchaus komplexe Aufgabe einfacher zu machen, gibt es auf der Website von HateAid Anleitungen für die verschiedenen Netzwerke. Und auch im Internet gibt es frei verfügbare Tools, um dem Screenshot einen Zeitstempel zu verpassen.

V. Welche Delikte kommen am häufigsten vor?

Es folgt ein kurzer Überblick über die Delikte, die uns am häufigsten in unserer Arbeit begegnen. Dabei geht es mir insbesondere um kleinere

Besonderheiten, die der Gesetzgeber kürzlich geändert hat, weil die Änderungsgründe unmittelbar mit dem Phänomen der digitalen Gewalt verknüpft sind.

1. Beleidigung, § 185 StGB, und verhetzende Beleidigung, § 192a StGB

Neu gesetzlich geregelt ist die verhetzende Beleidigung. Es handelt sich um eine Beleidigung, die sich nicht gegen ein Individuum als solches richtet, sondern gegen seine Zugehörigkeit zu einer Gruppe. Sie ist kein Antrags- und Privatklagedelikt, wovon wir uns mehr Strafverfolgung erhoffen. Sie greift etwa, wenn eine Person wegen ihrer sexuellen Orientierung oder ihrer religiösen Angehörigkeit herabgewürdigt wird. Leider wurde das Geschlecht als Kategorie nicht aufgenommen. Wir hätten uns dies gewünscht, weil wir überzeugt sind, dass es vor allem bei dem Thema der geschlechtsspezifischen digitalen Gewalt geholfen hätte.

Neuer Straftatbestand der verhetzenden Beleidigung: § 192a StGB

2. Üble Nachrede und Verleumdung, §§ 186, 187 StGB

Mit Blick auf die üble Nachrede möchte ich lediglich auf eine Besonderheit hinweisen, die auch im Internet gilt: Es ist unerheblich, ob man weiß, dass die verbreitete Behauptung nicht wahr ist oder ob sie wahr sein könnte oder ob man das für möglich hält. Wenn man selbst solche Beiträge verfasst oder eben auch „nur" teilt, was durch einen simplen Mausklick passieren kann, ist man im Zweifel schon strafbar, etwa wenn Falschzitate von Politiker*innen massenhaft geteilt werden. Auch hier lohnt sich also eine Meldung nach dem NetzDG und eine Strafanzeige.

3. Bedrohung, § 241 StGB

Früher bedurfte es der Androhung eines Verbrechens – das heißt einer Straftat, die mindestens mit einer Freiheitsstraße von einem Jahr geahndet werden kann. Diese hohe Strafbarkeitsschwelle wurde nun herabgesetzt: Nunmehr ist auch unter anderem die Androhung einer Vergewaltigung oder Körperverletzung strafbar. Hierdurch wurde eine wichtige Strafbarkeitslücke geschlossen.

4. Belohnung und Billigung von Straftaten, § 140 StGB

Auch die öffentliche Billigung einer bloß fiktiven Straftat im Internet ist nun strafbar

Das gleiche gilt für die Billigung von Straftaten im Netz, deren enger Anwendungsbereich vielfach missbraucht wurde. Ursprünglich griff § 140 StGB nämlich nur für den Fall, dass die Straftaten, auf die sie Be-

zug nehmen, auch begangen oder in strafrechtlich relevanter Weise versucht worden waren, etwa die Lobpreisung der Tötung des Kasseler Regierungspräsidenten Walter Lübcke. Nach der Änderung kann auch eine fiktive Straftat, die öffentlich zum Beispiel im Internet gebilligt oder gar bejubelt wird, hierunter fallen.

5. Volksverhetzung, § 130 StGB

Wenig Änderungen gab es am Tatbestand der Volksverhetzung. Hier stellen sich viele Fragen bei der Auslegung und die Strafbarkeitsschwelle ist sehr hoch. Trotzdem gibt es Äußerungen, die eindeutig darunterfallen, etwa im Bereich von rassistischen Beleidigungen oder antisemitischen Äußerungen. Besonders für den deutschen Rechtsraum ist, dass hier die Holocaust-Leugnung oder -Verharmlosung für sich genommen schon strafbar ist.

6. Verfassungsfeindliche Symbole, § 86a StGB

Der Verfassungsschutz gibt jedes Jahr eine Broschüre heraus, die auflistet, welche Symbole unter die „verfassungsfeindlichen Symbole“ im Sinne des § 86a StGB fallen. Diese Broschüre ist vor allem hilfreich, wenn man sich viel im Netz aufhält und gegebenenfalls einschlägige Inhalte melden möchte, da sie dabei hilft, Symbole wiederzuerkennen. Das Delikt kann relativ einfach verwirklicht werden, und wird von den Behörden gleichzeitig auch sehr ernst genommen. Die Meldung eines Hakenkreuzes kann dann schnell zu einer Hausdurchsuchung führen.

> Die Verwendung verfassungsfeindlicher Symbole wird von den Behörden sehr ernst genommen und verfolgt

VI. Was HateAid mit seiner Arbeit erreicht hat

Zum Abschluss möchte ich einige erfolgreiche Beispiele von Personen des öffentlichen Lebens anführen, in denen es sich gelohnt hat, gegen Hass im Netz aktiv zu werden. Es handelt sich um Erfolge von HateAid, die dazu geführt haben, dass auch andere Betroffene sich ermutigt gefühlt haben, selbst gegen das vorzugehen, was sie erleben.

> Die Erfolge von HateAid ermutigen andere Betroffene

Wir haben Luisa Neubauer dabei unterstützt, gegen den Rechtsextremisten Akif Pirinçci vorzugehen, der sie mehrfach auf übelste Weise sexistisch beleidigt hat. Er wurde verurteilt 6.000 € Geldentschädigung an Luisa Neubauer zu zahlen. Zwar ist das Urteil noch nicht rechtskräftig, aber für uns trotzdem als Erfolg zu verzeichnen.

Auch haben wir Renate Künast mehrfach unterstützt, unter anderem gegen den Rechtsextremisten Sven Liebich, der ein Falschzitat von ihr verbreitet hat und damit seine Follower*innen gegen sie aufhetzte. Weiterhin unterstützen wir Renate Künast in einem Verfahren gegen Facebook, in dem folgende Fragen geklärt werden sollen: Welche Pflichten hat Facebook? Muss Facebook, wenn ein Meme mit Falschzitat hundertfach geteilt wird, nur den einzelnen gemeldeten Post löschen, oder geht die Löschpflicht darüber hinaus? Denn die Betroffenen können gar nicht alles sehen, was gegen sie verbreitet wird. Oft befinden sich die Posts in geschlossenen Gruppen, auf privaten Profilen, sind hundertfach vorhanden.[10]

Den Pianisten Igor Levit haben wir unter anderem in einem Verfahren gegen Twitter unterstützt, in dem Auskünfte eingefordert werden sollten über Accountdaten der Menschen, die ihn, vor allem antisemitisch, beleidigt und bedroht haben.

Zuletzt ein für uns besonders schöner Erfolg: Durch unsere Unterstützung konnte erstmals ein Urteil gegen eine Online-Plattform erzielt werden, nach dem eine Geldentschädigung gezahlt werden musste. In diesem Fall hat Twitter extrem sexistische Kommentare, die bereits in einem vorangegangenen Gerichtsverfahren als Beleidigungen eingestuft wurden, was Twitter bekannt war, nicht gelöscht. Das Urteil ist zwar noch nicht rechtskräftig, aber ein ganz klares Zeichen hin zu mehr Verantwortung und Haftung für die Plattform.

Durch die Unterstützung von HateAid konnte erstmals ein Urteil gegen eine Online-Plattform erzielt werden

Natürlich sind die genannten Fälle nicht die einzigen Erfolge. Aber es sind die Erfolge, die uns vielleicht am meisten in Erinnerung geblieben sind.

Literatur

Bundeskriminalamt: Politisch motivierte Kriminalität im Jahr 2019. Bundesweite Fallzahlen, 12.5.2020, abrufbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2020/pmk-2019.pdf?__blob=publicationFile&v=6.

[10] LG Frankfurt a. M., Urteil vom 08.04.2022 – 2-03 O 188/21: Das LG Frankfurt a.M. hat inzwischen Facebook dazu verurteilt, alle Posts, die das Falschzitat enthalten, zu löschen und Renate Künast ein Schmerzensgeld in Höhe von 10.000 Euro zu zahlen. Facebook hat Berufung gegen das Urteil eingelegt.

Eckes, Christine / Fernholu, Tobias / Geschke, Daniel / Klaßen, Anja / Quent, Matthias: #Hass im Netz: Der schleichende Angriff auf unsere Demokratie. Eine repräsentative Studie in Hessen, hrsgg. vom Institut für Demokratie und Zivilgesellschaft, abrufbar unter https://www.idz-jena.de/fileadmin/user_upload/Bericht_Hass_im_Netz.pdf.

HateAid: Grenzenloser Hass im Internet – Dramatische Lage in ganz Deutschland, abrufbar unter https://hateaid.org/eu-umfrage-grenzenloser-hass-im-internet/#0-dramatische-lage-in-der-eu-jeder-zweite-junge-erwachsene-ist-selbst-betroffen.

HateAid: Bundesverfassungsgericht: Künast verbucht doch noch Erfolg im Facebook-Verfahren, 2.2.2022, abrufbar unter https://hateaid.org/bundesverfassungsgericht-kuenast-facebook-erfolg/.

Kreißel, Philip / Ebner, Julia / Urban, Alexander / Guhl, Jakob: Has Knopfdruck – Rechtsextreme Trollfabriken und das Ökosystem ko nierter Hasskampagnen im Netz, London 2018, abrufbar unte https://www.isdglobal.org/wp-content/uploads/2018/07/ISD_Ich_Bin_Hier_2.pdf.

IMPRESSIONEN AUS DER DISKUSSION…

„Wie gehen Sie eigentlich im Berufsalltag damit um, dass Sie ja doch bei ihrem Job immer mal wieder gegen Mauern laufen?“

„Ja, das ist richtig. Tatsächlich habe ich diese Mauern immer eher als Ansporn empfunden. Das ginge mir vielleicht anders, wenn ich einen anderen Beruf hätte und in diesem Kontext angefeindet werden würde und deswegen andauernd gegen meine eigenen Mauern rennen würde, aber da es ja mein Job ist, diese Mauern einzureißen, ist es tatsächlich eher ein Ansporn für mich, hier auch die Möglichkeit zu nutzen, mich auch mit Rechtsfragen zu beschäftigen, die noch völlig unbearbeitet sind und wo dann eben auch die Möglichkeit besteht, Betroffenen Wege aufzuzeigen, die sie für sich selber gar nicht gefunden haben – und da eben auch ein bisschen Kreativität walten zu lassen. Dieses ‚David gegen Goliath‘, wenn es vor allem gegen die Social-Media-Plattformen geht. Das ist natürlich auch etwas, wo wir das Privileg der Organisation haben – das ist natürlich auch ein hart verdientes Privileg, dass wir dann die Möglichkeit haben, Projekte aufzuziehen, für die wir dann Fördergelder kriegen, wodurch wir diese Klageverfahren führen können. Das ist natürlich auch etwas, was man nicht unterschätzen darf und was uns dann von Privatpersonen unterscheidet. Bei allem, was wir tun, sehen wir auch die Dimension, die über den Einzelfall hinausgeht, und haben immer im Kopf, dass wir hier an etwas arbeiten, was vielen Betroffenen helfen soll.“

„Braucht es eine Klarnamenpflicht oder reicht eine bessere Ausbildung im Rahmen der Strafverfolgung, um Täter*innen ausfindig zu machen?“

„Das wird jetzt gerade wieder sehr aktiv diskutiert, insbesondere deswegen, weil genau zu diesem Thema, nämlich zu der in den Allgemeinen Geschäftsbedingungen von Facebook verankerten Klarnamenpflicht – Facebook will eigentlich, dass die Nutzenden dort mit Klarnamen auftreten –, am Donnerstag vom Bundesgerichtshof entschieden wird. Dort wird ein Urteil in dieser Sache ergehen. Deswegen ist das ein Thema, worüber wir natürlich auch hier nachdenken, und ich muss sagen, auch wenn es die Strafverfolgung vielleicht verbessern könnte, sind wir natürlich gegen eine Klarnamenpflicht. Wir wollen nicht, dass Menschen gezwungen sind, mit

ihrem vollen Vor- und Zunamen aufzutreten. Ich habe es gerade in Endlosschleife gesagt, man darf nicht zu viele Informationen von sich preisgeben, und es ist auch überhaupt gar nicht notwendig, dass die ganze Welt den vollständigen Namen sehen kann. Was ich hingegen nicht verstehe, ist natürlich, wenn man dann sagt, es soll aber auch wirklich einen absoluten Anspruch auf Anonymität im Netz geben, egal was passiert. Denn ich finde dieser Anspruch sollte zumindest dann nicht bestehen, wenn schwere Straftaten begangen werden. Das heißt, es sollte doch für die Ermittlungsbehörden die Möglichkeit geben, herauszufinden, mit wem man es da zu tun hat, und das ist momentan eben nicht so einfach und auch durch Schulungen leider nicht so leicht umzusetzen. Also wenn wir alle Polizeibeamt*innen und Staatsanwält*innen im Land schulen würden, hätten wir trotzdem immer noch große Probleme, weil diese Unternehmen im Ausland sitzen und weil IP-Adressen nur fünf Tage gespeichert werden. Ich möchte jetzt auch gar keine Vorratsdatenspeicherung einführen, aber es gibt hier andere schlaue Vorschläge, wie man vorgehen könnte. Einer der radikaleren Vorschläge, aber einer, den ich ehrlich gesagt auch befürworte, ist, eine Verifizierungspflicht mit der Telefonnummer einzuführen. Viele Menschen geben von sich aus ihre Telefonnummer auf Social Media an, um die Zwei-Faktor-Authentifizierung zu nutzen, und das sind für die Ermittlungsbehörden sehr dankbare Daten, mit denen sie sehr gut arbeiten können. Die IP-Adresse schneller beauskunften zu können, ist natürlich auch ein Ansatz, den wir begrüßen und der sicherlich weniger eingriffsintensiv ist. Das heißt, es gibt hier andere Mittel und Wege. Im Idealfall gäbe es natürlich eine gesamteuropäische Lösung, die auch deutsche Ermittlungsbehörden befähigt, auf Daten von irischen Behörden zuzugreifen, denn die sitzen ja auf dem Datenschatz. Wenn die bei schweren Straftaten zumindest die Daten einfach herausgeben würden, hätten wir weniger Probleme."

„Neben Täter*innen mit einem hohen Organisationsgrad gibt es jedoch viele Personen – oft Rentnerinnen und Rentner - die mit Ihrem Klarnamen auftreten und offen strafrechtlich relevante Beiträge posten. Geht von solchen Täter*innen eine geringere Gefahr aus?"

„Mein Eindruck ist nicht, dass es 90 % derjenigen betrifft, die dann tatsächlich auch strafrechtlich verfolgt werden. Natürlich sind es die, die vielleicht am ehesten erwischt werden, das muss man auch sagen. Also ein Staatsanwalt sagte mal zu mir: ‚Wir erwischen nur die, die so doof sind, sich mit ihrem Kennzeichen auf Facebook abzulichten.' Also da ist dann halt auch was Wahres dran. Also diejenigen, die wirklich organisiert mit mehreren Profilen vorgehen, die passen dann natürlich auch ein bisschen auf, was sie von sich preisgeben. Jedoch nicht immer – es gibt auch dann verschiedene Kreuztreffer oder man findet doch mal die Bilder von irgendwas. Ich hatte auch schon Fälle, wo ich ein bisschen nachgeforscht habe, und bin ich dann tatsächlich auch auf ‚Das Örtliche' fündig geworden; die Person hatte noch bei ihrer Mutter gewohnt, das

war auf dann recht einfach. Aber viele, die extrem organisiert sind, machen das dann eben professioneller. Da kann man sich jetzt natürlich sagen: ‚Dann bringt das alles nichts'. Auf der anderen Seite zielt Abschreckung natürlich nicht nur auf diese Leute ab – auch, wenn man sie gerne kriegen würde. Sondern auch auf diejenigen, die sich davon vielleicht mitreißen lassen, die vielleicht dann der Meinung sind, sie könnten jetzt ihre dunkelsten Phantasien im Netz ausleben, weil das heutzutage wieder sagbar ist. Aber auch diejenigen spielen natürlich eine Rolle bei der Masse dessen, was wir auf Social Media sehen und deswegen lohnt es sich, auch sie zu verfolgen. Es stimmt schon, dass wir natürlich alles sehen: Vom hartgesottenen Rechtsextremisten bis zur Rentnerin; unser Lieblingsbeispiel ist die Hundesalonbesitzerin aus Süddeutschland, die aus allen Wolken gefallen ist und der eingefallen ist, dass sie eigentlich gar nicht so viel Geld hat, um jetzt die Geldstrafe zu bezahlen. Das passiert auch und das sind natürlich auch nicht die, die wir gerne bekommen wollen, aber die dann eben auch mit ins Netz gehen."

„Stichwort Täterinnen im Netz: Würden Sie sagen, dass Frauen die Emanzipation in diesem Deliktbereich im Negativen auch ein bisschen vorantreiben – oder sind es dann doch am Ende des Tages meistens wieder Männer?"

„Also es gibt auch Frauen, weibliche Täterinnen. Es gibt auch Frauen, die sich auf andere Frauen stürzen. Das passiert dann auch manchmal in so feministischen Debatten, wo man sich dann auch fragt, was jetzt eigentlich gerade schiefgelaufen ist, um mit dieser Situation dazustehen. Dennoch sagen die meisten Ermittlungsbehörden, dass es tendenziell ein Tick mehr Männer gibt. Bei der niedrigen Identifizierungsquote wissen wir aber auch gar nicht, wer hinter diesen Profilen überhaupt steht. Wir wissen, dass es auch einen Trend gibt, – weil es eben immer dieses Narrativ gibt, dass es vor allem Männer sind –, Fake Profile weiblich auszugestalten, damit es so aussieht, als wären es eben auch mehr Frauen. Wir können es aber einfach nicht sagen, es gibt keine belastbaren Zahlen zu diesem Thema, deswegen bin ich mit Mutmaßungen sehr vorsichtig. Vom Gefühl her sind es auch bei uns ein Tick mehr Männer in der Prozesskostenfinanzierung. Aber das ist natürlich auch nur ein Ausschnitt, also das hängt davon ab, wer findet den Weg zu uns, wer wird identifiziert und wer landet dann auch vor Gericht, weil er sich außergerichtlich nicht einigen konnte – da sind so viele Faktoren, die reinspielen, dass ich mir da kein Urteil zu anmaßen kann."

KÜNSTLICHE INTELLIGENZ IN DER STRAFVERFOLGUNG

LUDWIG BOTHMANN

Dr. Ludwig Bothmann, Wissenschaftlicher Mitarbeiter und Habilitand am Lehrstuhl für Statistical Learning & Data Science von Professor Dr. Bernd Bischl an der Ludwig-Maximilians-Universität München

Künstliche Intelligenz (KI) ist in aller Munde und auch im Bereich der Strafverfolgung gibt es erste Einsatzszenarien für KI. Dieser Beitrag verfolgt drei Ziele: Erstens sollen Leser*innen mit den Bedeutungen der Begriffe KI und maschinelles Lernen vertraut gemacht werden. Zweitens soll verständlich werden, wie die Qualität einer KI evaluiert werden kann, um (spätere) Staatsanwält*innen, Richter*innen oder ähnliche Personen in die Lage zu versetzen, informierte Entscheidungen über den Einsatz von KI treffen zu können. Drittens soll aufgezeigt werden, welche Schritte zur Entwicklung und Inbetriebnahme einer KI gehören, um ein Gefühl dafür zu vermitteln, in welchen Situationen der Einsatz von KI hilfreich sein könnte.

I. Einführung

Mit der Entwicklung von KI scheint ein großes Heilsversprechen verbunden zu sein. Sie wird benutzt, um die Coronapandemie zu bekämpfen[1]; ihr wird beigebracht, Computerspiele gut genug zu spielen, um professionelle menschliche Spieler*innen schlagen zu können[2]; sie wird zur Krebsdiagnose verwendet[3]; und natürlich spielt sie auch beim Thema autonomes Fahren eine große Rolle[4].

Die Entwicklung von KI ist mit einem Heilsversprechen verbunden

Auf der anderen Seite gehen mit diesem Heilsversprechen und mit dieser potenziell mächtigen technischen Neuerung auch viele Ängste einher: Ängste bezüglich der Einhaltung ethischer Prinzipien wie beispielsweise der Anwendung in einem System zur Gefühlserkennung der uigurischen Minderheit in China[5], über Fragen der Diskriminierungsfreiheit künstlicher Intelligenz[6] bis hin zur Furcht vor einer feindlichen Übernahme der KI[7]. Auf der einen Seite gibt es also viel Licht, auf der anderen Seite viel Schatten. Die Wahrheit liegt zwischen diesen Extremen. Wo dieses „Dazwischen" genau liegt und was es bedeutet, wollen wir im Folgenden herausarbeiten.[8]

1 *Lovell*, BioNTech and InstaDeep join forces to predict high-risk COVID variants, healthcareitnews.com.
2 *Schulz*, DeepMind-KI schlägt Starcraft-Profis, gamestar.de.
3 *Urbanek*, Künstliche Intelligenz versus Ärzte. Wer Brustkrebs besser diagnostiziert, Ärztezeitung.
4 *Jiru,* Autonomous Driving, Fraunhofer IKS.
5 *Reuter*, China teste Gefühlserkennung an uigurischer Minderheit, netzpolitik.org.
6 *Metz*, Who Is Making Sure the A.I. Machines Aren't Racist? New York Times.
7 *Cellan-Jones,* Stephen Hawking warns artificial intelligence could end mankind, bbc.
8 Eine sehr zu empfehlende Einstiegslektüre in das Thema ML ist auch das Buch von *Kersting/Lampert/Rothkopf*, Wie Maschinen lernen – Künstliche Intelligenz verständlich erklärt, Berlin 2019.

II. Begriffsklärung und Einsatzgebiete von KI

Künstliche Intelligenz – was bedeutet das? Man kann KI als Oberbegriff für Anwendungen ansehen, bei denen Maschinen menschenähnliche Intelligenzleistungen erbringen beziehungsweise menschliche Intelligenz in irgendeiner Weise imitieren[9]. Ein Kernelement der KI ist das maschinelle Lernen (ML) – in der Alltagssprache wird KI meist synonym für ML verwendet. Bei ML geht es darum, aus einer bestimmten Menge an Daten (im Folgenden auch „Trainingsdaten" genannt) Zusammenhänge zu lernen oder Muster zu finden, die man im Folgenden auf neue Daten anwenden kann. Im Zentrum von ML stehen also immer Daten, aus denen gelernt werden soll. Ein weiteres aktuelles Buzzword ist „Deep Learning". Deep Learning[10] ist eine von vielen Methoden des maschinellen Lernens und nutzt neuronale Netze, um die oben erwähnten Zusammenhänge aus den Daten zu lernen. Wir werden hier auf diese Methode nicht eingehen; es genügt zu wissen, dass Deep Learning ein Teilgebiet von ML ist.

Ein Kernelement der KI ist das maschinelle Lernen

1. Omnipräsente KI

Uns allen begegnet KI regelmäßig im Alltag, und zwar ohne, dass uns das zwingend auffallen würde. Ein Beispiel sind sogenannte „Recommender Systems"[11], also Vorschlagssysteme, die uns weitere Artikel vorschlagen, nachdem wir eine Serie angesehen, ein Produkt in einem Onlineshop gekauft oder ein Musikstück gestreamt haben. Anwendungen von Gesichtserkennungssystemen nutzen wir zur Entsperrung unserer Smartphones[12]. Und auch wenn wir ein Onlinetool zur Übersetzung verwenden, nutzen wir die Vorteile von KI.[13]

2. Erfolgsvoraussetzungen

Wie sehen die Erfolgsvoraussetzungen für einen Einsatz von KI aus? Der zentrale Erfolgsfaktor sind die Daten, mit denen die KI trainiert wird, denn eine Maschine lernt nicht einfach von sich aus „selbstständig" – auch wenn man diesen Eindruck in der aktuellen Berichterstattung teils gewinnen kann. Eine Maschine lernt ausschließlich aus Daten und kann deshalb nie mehr wissen als das, was in diesen Trainingsdaten

Zentraler Erfolgsfaktor sind die Daten, mit der die KI trainiert wird

---

9 Europäisches Parlament, Was ist künstliche Intelligenz und wie wird sie genutzt?.

10 Siehe z.B. das Buch von *Goodfellow/Bengio/Courvilleet*, Deep Learning, Cambridge 2016.

11 *Seif*, An Easy Introduction to Machine Learning Recommender Systems, KDnuggets.com.

12 Siemens-Stiftung, Praxisbeispiel: Gesichtserkennung, 2019.

13 *Fulterer*, Warum automatische Übersetzer so gut funktionieren, nzz.de.

steckt – „garbage in – garbage out“. Was heißt es aber nun, „gute“ Daten zu haben? Zunächst einmal bedeutet es, genug Daten zu haben, Stichwort „Big Data“. Die *Quantität* allein ist aber noch nicht alles; wir brauchen auch *qualitativ* hochwertige Daten. Dieser Gesichtspunkt lässt sich in zwei Aspekte aufspalten: Der erste Punkt ist, dass die Trainingsdaten ungefähr den Produktionsdaten entsprechen. Trainingsdaten sind hierbei die Daten, mit denen die Maschine lernt (als Endprodukt ergibt sich ein ML-Modell), und Produktionsdaten sind die Daten, auf die das gelernte ML-Modell später angewendet wird. Wenn also eine KI entwickelt werden soll, die Bilder von Hunden und Katzen unterscheidet, bestehen die Trainingsdaten aus einer großen Menge von Bildern von Hunden und Katzen und zum Produktionszeitpunkt sollen neue Bilder in diese beiden Klassen eingeordnet werden. Diese Bilder sollten den Trainingsdaten ähnlich sein, also gleiche Arten von Hunden und Katzen zeigen, ähnliche Hintergrundmotive und Beleuchtung etc., da das ML-Modell andernfalls schlechte Ergebnisse liefern wird. Der zweite Punkt ist, dass wir Beispiele aller Klassen brauchen, die zum Produktionszeitpunkt erwartet werden. Wenn nur auf Hunde und Katzen trainiert wurde und zur Produktionszeit auf einmal ein Bild erscheint, das weder einen Hund noch eine Katze zeigt, dann weiß die KI nicht, was sie machen soll, weil sie so etwas noch nie gesehen hat: Da ihre Welt nur aus Hunden und Katzen besteht, wird sie das Bild dennoch als Hund oder Katze einordnen, obwohl beides falsch ist.

Man unterscheidet zwischen Trainingsdaten und Produktionsdaten

3. Spektakuläre Fälle von KI-Versagen

Es gibt einige Fälle von sehr spektakulärem KI-Versagen. Oft drehen sich diese Fälle um diskriminierendes Verhalten, teilweise auch um fatale Fehlentscheidungen. Im Folgenden erläutern wir anhand zweier Beispiele, wieso die jeweilige KI ein diskriminierendes Verhalten an den Tag legte, und betrachten im Anschluss ein Beispiel für eine fatale Fehlentscheidung.

Im ersten Beispiel entwickelte eine Firma eine Recruiting-KI.[14] Die Idee war, eine Maschine die Bewerbungen vorfiltern zu lassen und nur die vielversprechendsten an Menschen aus der Personalabteilung weiterzuleiten, um somit den Einstellungsprozess effizienter zu gestalten. Wenn nun aber die KI mit historischen Daten trainiert wird (und andere Daten als historische Daten gibt es natürlich nicht), frühere Einstellungsentscheidungen diskriminierend waren und die KI Zusammenhänge aus diesen Daten lernen soll, dann lernt die KI genau diese Diskriminierung

[14] Application Security Series, Top 10 Failures of AI, immuniweb.com.

und reproduziert dieses Verhalten – ein Fall von„garbage in – garbage out“.

Ähnlich gelagert ist der Fall eines Twitterbots,[15] der entwickelt wurde, um beispielhaft das Potential einer KI zu zeigen. Dieser Twitterbot sollte im Gespräch mit menschlichen Twitternutzer*innen lernen, wie ein Mensch zu sprechen, und anschließend eigenständig Tweets verfassen. Das Ergebnis war, dass sich dieser Twitterbot nach kürzester Zeit zu einer rassistischen, sexistischen, faschistischen Meinungsmaschine entwickelte, sodass er bereits nach 16 Stunden wieder deaktiviert wurde. Wie konnte dieser Twitterbot ein solches Verhalten entwickeln? Wahrscheinlich hat er viele derartige Tweets als Vorbilder gesehen (möglicherweise wurde er auch gezielt von Trolls in diese Richtung „gefüttert“) und daraus gelernt, dass dies „normale menschliche Sprache“ ist. Eine KI hat kein Moralverständnis, sie lernt einfach aus Daten.

Eine KI hat kein Moralverständnis, sie lernt einfach aus Daten

Ein anderer Fall von spektakulärem KI-Versagen betrifft eine fatale Fehlentscheidung – einen tödlichen Unfall mit einem selbstfahrenden Auto.[16] Hier liegt die Sache allerdings etwas anders als bei den Beispielen des diskriminierenden Verhaltens: Es ist nämlich nicht zwingend, dass hier die Trainingsdaten zu schlecht oder zu wenig umfangreich waren. Vielmehr ist es so, dass eine (auch noch so gut trainierte) künstliche Intelligenz genauso wenig perfekt ist wie ein Mensch. Derartige Unfälle können also nicht mit Sicherheit ausgeschlossen werden, wenn man beschließt, einer KI die entsprechende Entscheidungsmacht zu übertragen. Natürlich kann aus einem einzelnen Unfall nicht geschlossen werden, was gefährlicher ist: ein menschlich gesteuertes Auto oder ein selbstfahrendes Auto.

Was ist gefährlicher? Ein menschlich gesteuertes oder ein selbstfahrendes Auto?

III. Crashkurs Machine Learning

Nach der Begriffsklärung und einigen einleitenden Beispielen wollen wir nun eine Ebene tiefer gehen – für einen Crashkurs in ML.[17] Wir werden sehen, welche Schritte zu einem ML-Anwendungsfall gehören und wie man ein ML-Modell evaluieren kann.

15 *Beuth,* Twitter-Nutzer machen Chatbot zur Rassistin, zeit.de.

16 *Hawkins,* Uber is at fault for fatal self-driving crash, but it's not alone, theverge.com.

17 Für eine ausführliche Einführung siehe neben *Kersting/Lampert/Rothkopf*, Wie Maschinen lernen – Künstliche Intelligenz verständlich erklärt, Berlin 2019; auch *James et al.,* An Introduction to Statistical Learning – with Applications in R, Berlin 2021.

1. Lernprozess vs. Prognose

Vorhersage der Rückfallwahrscheinlichkeit von Personen, die Straftaten begangen haben, durch ein ML-Modell

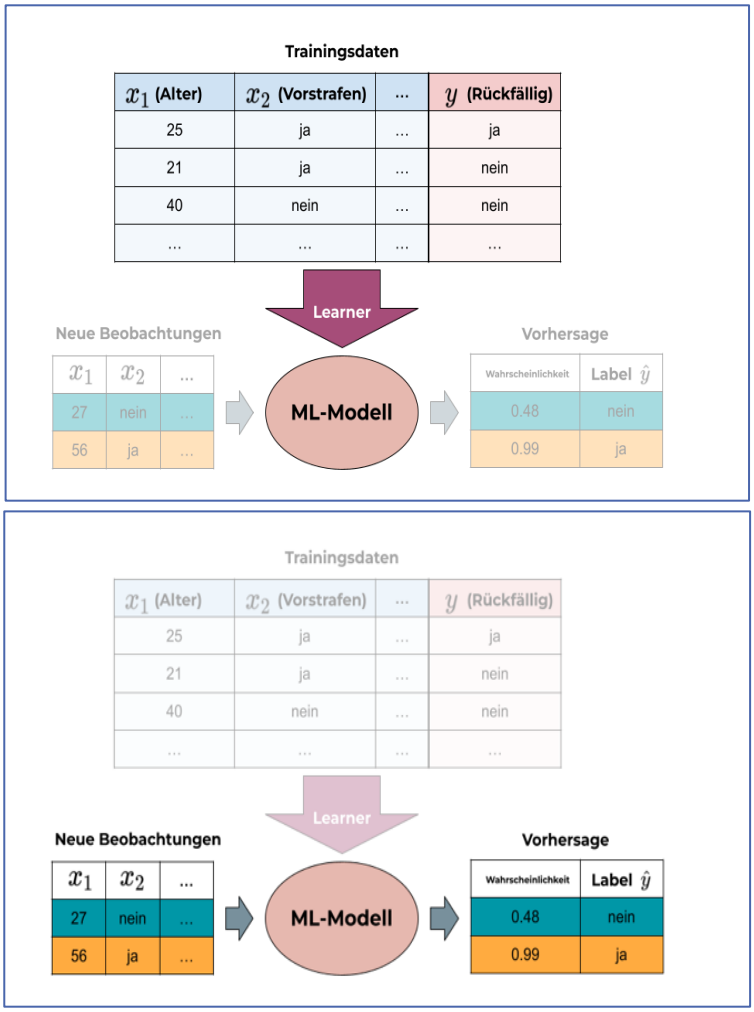


Abbildung 1: Lernprozess (oben) und Prognose (unten)

Wir beginnen mit den schon mehrmals erwähnten Trainingsdaten in Form einer Tabelle mit Zeilen und Spalten (s. Abbildung 1 (oben) „Trainingsdaten"). Jede Zeile entspricht einer Person und die Einträge einer Zeile bilden Eigenschaften der jeweiligen Person ab, hier das Alter der Person (x1), einen binären Indikator, ob diese Person vorbestraft ist (x2), und potentiell weitere Variablen (hier mit „…" angedeutet). In der letzten Spalte (ganz rechts) steht zudem eine anders eingefärbte Variable y, die beschreibt, ob diese Person später (bis zu zwei Jahre nach einer Verurteilung) rückfällig geworden ist oder nicht.[18] Die mit x bezeichneten Variablen werden auch Features oder Kovariablen genannt; die mit y bezeichnete Variable wird Zielvariable, Response oder Target genannt.

[18] *Angwin/Larson/Mattu/Kirchner,* Machine bias: There's software used across the country to predict future criminals. and it's biased against blacks, ProPublica.org.

In diesem beispielhaften Anwendungsfall soll vor Gericht vorausgesagt werden, ob eine angeklagte Person wieder rückfällig werden wird oder nicht, um basierend darauf über gewisse Maßnahmen zu entscheiden (z.B. Kaution, Bewährung, etc.). Die Frage ist also, wie wahrscheinlich es ist, dass eine Person rückfällig wird. Hierfür werden im ersten Schritt (historische) Trainingsdaten gesammelt, bei denen alle Features x und das Target y bekannt sind (dies könnte das Ergebnis einer Datenbankabfrage sein). Aus diesen Daten soll ein Zusammenhang gelernt werden zwischen Target y und Features x; dieser Zusammenhang hat eine funktionale Form und wird oft mit f(x) beschrieben. Die Rückfallwahrscheinlichkeit ist also eine Funktion der Features (Alter, Vorstrafen, usw.), die aus den Trainingsdaten gelernt werden soll. Hierzu empfängt ein Algorithmus, der auch „Learner" genannt wird, als Input die Trainingsdaten; Output des Learners ist dann das gelernte ML-Modell f(x) (s. Abbildung 1 (oben)).

Betrachten wir nun den Prognosezeitpunkt (s. Abbildung 1 (unten)): Zum Prognosezeitpunkt erhält das ML-Modell als Input die Daten von neuen Personen, von denen die Features bekannt sind (Alter, Vorstrafen, usw.), aber nicht das Target y, also die Information, ob die Person rückfällig werden wird. Nun wird die vorher gelernte Funktion f(x) auf die neuen Daten angewendet. Ergebnis ist eine vorhergesagte Rückfallwahrscheinlichkeit für jede neue Person, im Beispiel für zwei Personen 48 % bzw. 99 %. Im weiteren Prozess kann man nun entweder direkt mit der Wahrscheinlichkeit fortfahren oder eine binäre Entscheidung verlangen: Wenn die Wahrscheinlichkeit über einem bestimmten Grenzwert ist, wird „ja" vorhergesagt, andernfalls „nein". Man könnte alternativ auch einen mehrstufigen Risikoscore entwickeln. Wichtig zu verstehen ist: Was aus dem ML-Modell in erster Linie herauskommt, ist die vorhergesagte Wahrscheinlichkeit; die Weiterverarbeitung hiervon kann durch die Nutzer*innen von Fall zu Fall variieren.

Dieses Konzept von Lernen und Vorhersagen ist das Herzstück maschinellen Lernens: Aus Trainingsdaten (bestehend aus Features x und Target y) wird ein Zusammenhang bzw. ein Modell f(x) gelernt und zum Prognosezeitpunkt wird dieses Modell f(x) auf neue Daten (ausschließlich Features x) angewendet, um das dort unbekannte Target y vorherzusagen.

Dieses Konzept von Lernen und Vorhersagen ist das Herzstück von maschinellem Lernen

2. Entwicklung / Anwendung eines ML-Modells

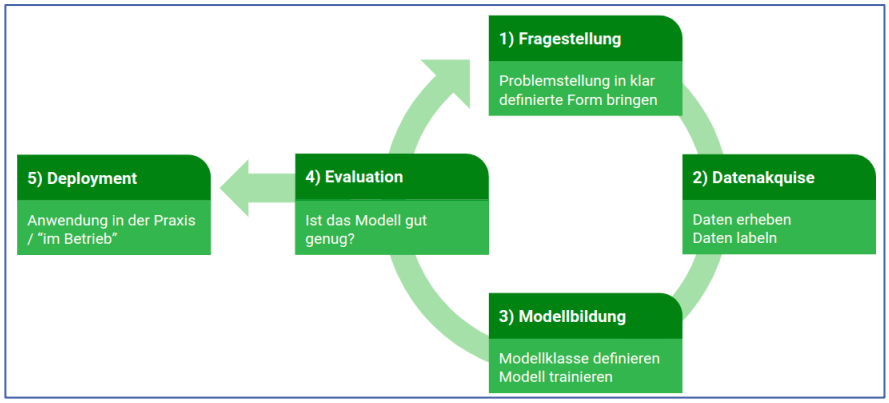


Abbildung 2: Kreislauf der Entwicklung und Anwendung eines ML-Modells

Abbildung 2 stellt den Kreislauf von Entwicklung und Anwendung eines ML-Modells dar. Als Erstes muss die zu beantwortende Fragestellung, die Problemstellung, in eine klar definierte Form gebracht werden. Nur eine eindeutig definierte Frage kann auch klar und eindeutig beantworten werden. Im obigen Beispiel könnte die Problemstellung wohl lauten: „Vorhersage der Rückfallwahrscheinlichkeit anhand der Features Alter, Vorstrafen, etc.“. Natürlich müsste hier die gesamte Menge der Features konkret benannt werden; zudem sollte der Begriff der Rückfallwahrscheinlichkeit genauer definiert werden, z.B.: Innerhalb welchen Zeitrahmens? Bezogen auf welche Delikte? Für welchen Personenkreis?

Im zweiten Schritt müssen Daten erhoben werden. Im Beispiel der Rückfallwahrscheinlichkeit hieße das möglicherweise, eine bestimmte Datenbankabfrage zu starten. Zusätzlich müssen die Daten „gelabelt“ werden. Für jedes Individuum im Trainingsdatensatz muss also der wahre Wert des Targets y gefunden werden. Das mag in diesem Fall einfach sein, weil die Information darüber, ob eine Person rückfällig wurde, möglicherweise auch in der Datenbank zu finden ist. In anderen Anwendungsfällen kann das allerdings ein sehr zeitaufwändiger Prozess sein. Zum Beispiel bei Bilderkennungsproblemen müssen die Label, also die wahren Klassen der Bilder, oft manuell hinzugefügt werden. Das ist im Übrigen genau der Punkt, an dem „die Intelligenz in die KI kommt“: Es ist menschliche Intelligenz, die diese Bilder labelt und dann in den Trainingsprozess sendet.

> Die Datenerhebung stellt in der Praxis oftmals einen zeitaufwändigen Prozess dar

Schritt drei (Modellbildung) ist genau der Lernprozess, den wir oben beschrieben haben, an dessen Ende ein trainiertes ML-Modell steht. Hier wird entschieden, welche Art von Modellklasse verwendet soll: Eine mögliche Wahl ist ein tiefes neuronales Netz, also eine Methode

des Deep Learning, aber es existieren noch viele weitere Modellklassen wie „Classification and Regression Trees“[19], „Random Forests“[20], „Gradient Boosted Trees“[21], „Support Vector Machines“[22] u.v.m.

Bei Schritt vier, der Evaluation, steht die Frage im Mittelpunkt, wie „gut“ das ML-Modell ist (Details hierzu folgen im nächsten Abschnitt). Wenn das Modell nicht gut genug ist, beginnt der Kreislauf von vorne und jeder Schritt kann auf den Prüfstand kommen. Möglicherweise war die Problemstellung zu komplex und sie muss stärker eingegrenzt werden; oder sie war nicht ausreichend klar formuliert. Vielleicht war aber auch die Datenbasis nicht informativ genug, um die Problemstellung befriedigend lösen zu können – sei es, weil zu wenige Daten vorhanden waren, die Datenqualität nicht hoch genug war oder schlicht falsche Daten verwendet wurden. Es könnte zudem sein, dass die Modellklasse falsch gewählt wurde, technische Fehler passierten oder der Programmcode fehlerhaft war, der zum Modelltraining genutzt wurde.

Diesen Kreislauf muss man also gegebenenfalls mehrfach beschreiten, bis entschieden werden kann, das Modell im letzten Schritt „in Produktion zu bringen“, also in der Praxis anzuwenden (auch „Deployment“ genannt). In vielen Fällen wird das produktive ML-Modell mehr eine Entscheidungshilfe sein als eine alleinige Entscheidungsinstanz. Im Beispiel der Rückfälligkeit wird natürlich nicht basierend auf der Rückfallwahrscheinlichkeit, die ein ML-Modell vorhergesagt hat, eine Person in Haft geschickt. Vielmehr wird ein Mensch unter Zuhilfenahme dieser Information eine Entscheidung treffen.

Meist ist die KI Entscheidungshilfe, nicht Entscheidungsinstanz

3. Evaluation der Qualität eines ML-Modells

Wir wollen uns nun intensiver mit der Frage beschäftigen, wie ein ML-Modell evaluiert werden kann. Hierzu betrachten wir die Fehlerraten des ML-Modells. Basierend auf einer Confusion Matrix (s. Abb. 3), welche die korrekten und falschen Vorhersagen für einen sogenannten „Testdatensatz“ – also einen Datensatz, der ausschließlich Beobachtungen enthält, die beim Modelltraining nicht benutzt wurden – beschreibt, können viele unterschiedliche Arten von Fehlerraten definiert werden. Drei von diesen Fehlerraten werden wir hier näher betrachten, da diese die verschiedenen Interpretationen aus unserer Sicht gut beschreiben.

Für die Evaluierung des ML-Modells werden die Fehlerraten betrachtet

19 *Breiman et al.*, Classification and Regression Trees, New York 1984.
20 *Breiman*, Random Forests, Machine Learning 2001.
21 *Chen/Guestrin*, A Scalablae Tree Boosting System, Association for Computing Machinery 2016.
22 *Boser/Guyon/Vapnik,* A training algorithm for optimal margin classifiers, New York 1992.

Es ist aber wichtig festzuhalten, dass es viele verschiedene Fehlerraten gibt und dass je nach Anwendung unterschiedliche Fehlerraten wichtiger sind.

Betrachten wir zunächst die Confusion Matrix in Abb. 3: Die vier Werte in der Matrix beschreiben die vier möglichen Kombinationen aus wahrer Klasse y („+“ oder „-“) und vorhergesagter Klasse $\hat{y}$ („+“ oder „-“). Die linke Spalte enthält alle Fälle, die in Wahrheit zur positiven Klasse gehören. Die rechte Spalte enthält alle Fälle, die in Wahrheit zur negativen Klasse gehören. Analog enthält die erste Zeile alle Fälle, die als positiv vorhergesagt wurden, und die zweite Zeile alle Fälle, die als negativ vorhergesagt wurden. Üblicherweise werden die beiden Klassen als „positiv“ und „negativ“ bezeichnet, was keine Wertungsaussage beinhaltet, sondern schlicht die beiden Klassen unterscheidet (ähnlich zu einem positiven oder negativen Coronatest). Im Beispiel könnte „rückfällig = positiv“ und „nicht rückfällig = negativ“ gesetzt werden.

Die wahre Klasse y wird mit der vorhergesagten Klasse $\hat{y}$ verglichen

In zwei Fällen ist die Vorhersage korrekt, in zwei Fällen nicht: Wenn eine Person, die später rückfällig werden wird, als positiv vorhergesagt wird, ist die Vorhersage korrekt, dieser Fall wird als „true positive“ bezeichnet. Wenn eine Person, die später nicht rückfällig werden wird, als negativ vorhergesagt wird, ist die Vorhersage ebenfalls korrekt, dieser Fall wird als „true negativ“ bezeichnet. Die Fälle inkorrekter Vorhersagen werden analog mit „false positive“ (Person ist negativ, wird aber als positiv vorhergesagt) bzw. „false negative“ (Person ist positiv, wird aber als negativ vorhergesagt) bezeichnet.

		True Class y	
		+	−
Predicted Class $\hat{y}$	+	True Positive (TP)	False Positive (FP)
	−	False Negative (FN)	True Negative (TN)

Abbildung 3: Confusion Matrix

Diese vier Fälle können wir nun mit Zahlen unterlegen, siehe Abbildung vier: Es gibt 99 + 1 = 100 positive Fälle und 99 + 9801 = 9900 negative Fälle.

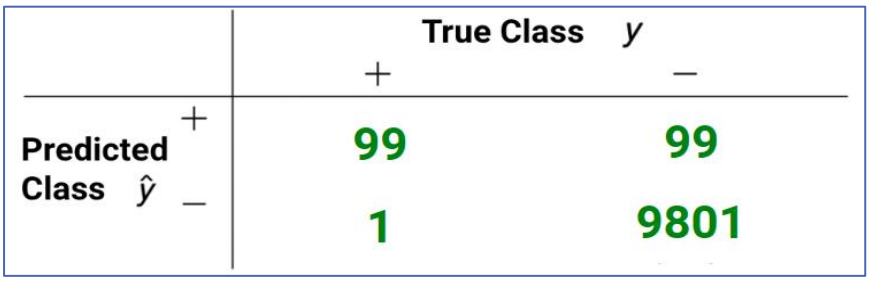


Abbildung 4: Confusion Matrix mit beispielhaften Zahlen

Anhand dieser Zahlen lassen sich beispielhaft die folgenden drei Fehlerraten berechnen:

- Precision = Anteil der tatsächlich Positiven an denen, die als positiv klassifiziert wurden = TP/(TP + FP)
- Recall = Anteil der als positiv Klassifizierten an denen, die tatsächlich positiv sind = TP/(TP + FN)
- Accuracy = Anteil der insgesamt korrekt Klassifizierten = (TP + TN)/(TP + FP + TN + FN)

Die verschiedenen Fehlerraten lassen sich durch Precision, Recall und Accuracy abbilden

Bei der Precision werden als Bezugsgröße diejenigen gewählt, die positiv klassifiziert wurden (TP und FP, also die erste Zeile); diejenigen, die als negativ klassifiziert wurden, spielen keinerlei Rolle. Die Precision ist dann der Anteil der Positiven an diesen Fällen. Der Blick geht also sozusagen in Zeilenrichtung: Bedingt auf die Vorhersage wird danach gefragt, wie häufig die Vorhersage richtig war.

Beim Recall geht der Blick hingegen in Spaltenrichtung. Bezugsgröße sind diejenigen, die tatsächlich positiv sind (TP und FN, also die erste Spalte); die in Wahrheit Negativen spielen keine Rolle. Der Recall ist dann der Anteil der als positiv Klassifizierten an diesen Fällen.

Abschließend bildet die Accuracy alle vier Werte der Tabelle in einer Metrik ab: Die Accuracy ist der Anteil der korrekt Klassifizierten an allen Vorhersagen.

Für diese Begriffe gibt es teilweise auch andere Bezeichnungen, die aber genau das Gleiche meinen. Sensitivität ist ein alternativer Begriff für den Recall und die Precision wird auch „Positive Predictive Value“ genannt. Darüber hinaus gibt es auch noch andere Fehlerraten, mit denen wir uns hier aber nicht weiter aufhalten wollen. Stattdessen rechnen wir die Werte dieser drei Fehlerraten für das Zahlenbeispiel in Abb. 4 aus und werden sehen, dass diese Fehlerraten für ein und dasselbe Modell sehr unterschiedlich sein können.

Für diese Begriffe gibt es auch andere Bezeichnungen, die aber das Gleiche meinen

Die Accuracy ist (99 + 9801)/(10000) = 99 %, der Recall ist mit 99/(99 + 1) = 99 % ebenfalls relativ hoch, die Precision hingegen mit 99/(99 + 99) = 50 % eher klein. Wie kommt es, dass die Accuracy und der Recall so hoch sind und die Precision so niedrig? In diesem fiktiven Beispiel liegt es daran, dass die negative Klasse viel öfter (9900 mal) vorkommt als die positive Klasse (100 mal), wir es also mit einem stark unbalancierten Datensatz zu tun haben. Hierbei handelt es sich um ein in der Praxis häufig auftretendes Phänomen, z.B. bei der Diagnose seltener Krankheiten. Es gibt also nur wenige positive Fälle und viele negative Fälle. Wenn ein Modell nun schlicht immer die negative Klasse voraussagt, landet man bei einer guten Accuracy, obwohl das Modell keine echte Information enthält; konsequenterweise ist die Precision sehr gering. Bei einem unbalancierten Datensatz können diese Fehlerraten daher sehr weit auseinander liegen. Es ist deshalb sehr wichtig, gut zu überlegen, welche Fehlerrate im konkreten Anwendungsfall wichtig ist.

Die Fehlerraten können bei ein und demselben Modell stark variieren

Mit einem gedanklichen Bild kann man sich hoffentlich besser vorstellen und merken, was Precision und Recall bedeuten. Bei der Precision kann man sich eine Scharfschützin vorstellen: Wann wird eine Scharfschützin eingesetzt? Sicherlich eher selten – aber wenn sie eingesetzt wird, ist eine hohe Zielgenauigkeit sehr wichtig: Sie soll auf den Befehl hin, eine Person zu treffen, erstens sicher treffen und zweitens auch genau die Person treffen, die sie treffen soll. Bezogen auf das ML-Modell heißt das: Wenn die positive Klasse vorhergesagt wird, dann soll diese Prognose auch wirklich stimmen – dafür nimmt man in Kauf, viele in Wahrheit Positive zu übersehen (sie also als negativ vorherzusagen).

In manchen Anwendungsfällen ist die Precision am wichtigsten

Beim Recall kann man an die Stecknadel im Heuhaufen denken: Wir haben einen Heuhaufen, in dem ein paar Stecknadeln sind und wir können nach und nach einzelne Elemente aus dem Heuhaufen ziehen (also entweder einen Grashalm oder eine Stecknadel). Ziel ist es, möglichst alle Stecknadeln aus diesem Heuhaufen herauszuziehen. Hierbei ist es nicht weiter schlimm, wenn man als Beifang eine gewisse Menge Grashalme herauszieht, solange am Ende alle Stecknadeln gezogen wurden. Bezogen auf das ML-Modell heißt das: Möglichst alle Positiven sollen auch als positiv klassifiziert werden – dafür nimmt man in Kauf, viele Negative auch als positiv zu klassifizieren. Als Zahlenbeispiel: Wenn in dem Heuhaufen 10 Stecknadeln sind und wir ziehen 100 mal und haben danach die 10 Stecknadeln gefunden, dann liegt die Precision bei 10 %, aber der Recall bei 100 %.

In anderen Fällen ist ein hoher Recall wichtiger

Betrachten wir ein neues Beispiel: Mord. Die wahre Klasse beschreibt, ob die Person einen Mord begangen hat (positiv) oder nicht (negativ). Die vorhergesagte Klasse beschreibt, ob sie wegen Mordes verurteilt wurde (positiv klassifiziert) oder nicht (negativ klassifiziert). Wie können Accuracy, Precision und Recall hier sprachlich abgebildet werden?

- Precision: Anteil derjenigen, die einen Mord begangen haben, an den Menschen, die wegen Mordes verurteilt wurden. Wenn jemand verurteilt wird, dann soll der Mordvorwurf auch stimmen.
- Recall: Anteil der wegen Mordes Verurteilten an den Menschen, die einen Mord begangen haben. Bezugsgröße sind diejenigen, die einen Mord begangen haben; wir wollen also „alle Stecknadeln im Heuhaufen" finden.
- Accuracy: Anteil derjenigen, die korrekterweise verurteilt bzw. freigesprochen wurden.

Die verantwortlichen Personen müssten sich jetzt die Frage stellen, welche dieser drei Metriken für sie die entscheidende ist. Dabei ist zu beachten, dass es sich möglicherweise um ein stark unbalanciertes Problem handelt, da es deutlich weniger Menschen gibt, die schon mal einen Mord begangen haben, als Menschen, bei denen das nicht der Fall ist. Wenn die Datengrundlage allerdings nur aus Menschen besteht, die wegen Mordes angeklagt sind, kann die Situation schon ganz anders aussehen und der Anteil derer, die einen Mord begangen haben, deutlich erhöht sein.

IV. KI in der Strafverfolgung

Nachdem beschrieben wurde, wie die Qualität eines ML-Modells beurteilt werden kann, soll im Folgenden ein Gefühl dafür vermittelt werden, in welchen Situationen der Einsatz von ML vielversprechend sein könnte. Wir ziehen dazu drei fiktive Einsatzszenarien aus dem Bereich der Strafverfolgung heran:

1. Entdeckung von Kinderpornographie: Kann mittels einer KI kinderpornographisches Material auf einem Laptop oder anderen Datenträgern eines Beschuldigten entdeckt werden?
2. Lügendetektor: Kann basierend auf einer Videoaufnahme einer Zeugenbefragung per KI entschieden werden, ob die Person gelogen hat oder nicht?

3. Entdeckung von Hate Speech: Kann Hate Speech auf einer Social-Media-Plattform per KI entdeckt werden?

Für diese drei Anwendungsfälle gehen wir nun den Kreislauf der Entwicklung eines ML-Modells durch und überlegen, was für eine Implementierung dieses Anwendungsfalls nötig wäre.

1. Entdeckung kinderpornographischen Materials

Entdeckung kinderpornographischen Materials als potentiell vielversprechender Anwendungsfall von ML

Betrachten wir noch einmal den Kreislauf in Abbildung 2: Als erstes muss die Problemstellung in eine klar definierte Form gebracht werden, d.h. es muss entschieden werden, worum es genau geht. Wollen wir Bilder entdecken oder Videos oder beides? Haben die Videos eine Tonspur oder nicht? Nehmen wir beispielhaft eine Festlegung auf Bilder an: Was genau gilt als kinderpornographisches Bild? Zählt hierzu schon die Zurschaustellung kindlicher Nacktheit? Was genau sind die Merkmale, die ein kinderpornographisches Bild von einem nicht kinderpornographischen Bild unterscheiden, gerade bei Grenzfällen?

Im zweiten Schritt müssen genügend Daten gesammelt werden (Trainingsdaten und Testdaten) und zwar realistische Daten – realistisch in dem Sinne, dass sie abbilden, was „in Produktion“ erwartet wird. Zum einen brauchen wir Positivbeispiele (also kinderpornographisches Material), zum anderen Negativbeispiele (also Bilder, die kein kinderpornographisches Material darstellen) und Grenzfälle. Besonders die Menge und Diversität der Grenzfälle kann erfolgsentscheidend sein. Alle Bilder müssen manuell gelabelt werden. Menschen müssen also für jedes Bild entscheiden, ob es sich um Kinderpornographie handelt oder nicht.

Im dritten Schritt wird das ML-Modell schließlich trainiert. Da es sich um die Klassifikation von Bilddaten handelt, bietet sich etwa ein Convolutional Neural Network an, eine spezielle Klasse aus dem Bereich des Deep Learning.

Hier wäre das Ziel wohl ein möglichst hoher Recall

Im vierten Schritt erfolgt die Modellevaluation. Hier stellt sich die Frage, bezüglich welchen Kriteriums das Modell evaluiert werden soll, also z.B. bezüglich Precision oder Recall. Hohe Precision hieße: möglichst jedes Bild, das die KI als Kinderpornographie labelt, ist tatsächlich auch kinderpornographisch. Hoher Recall hieße, möglichst alle kinderpornographischen Bilder zu finden. Möglicherweise wird die Entscheidung hier auf einen hohen Recall fallen, weil hinter jedem Bild eine potentielle

Straftat steckt. Anders gewendet: Wenn ein paar Bilder selektiert werden, die in Wahrheit nicht kinderpornographisch sind, ist das in diesem Fall eher nicht schlimm, da am Ende ohnehin ein Mensch diese Bilder nachkorrigiert.

Zusammenfassend scheint dies ein potentiell vielversprechender Anwendungsfall von ML zu sein, da es um eine sehr repetitive Tätigkeit geht: Die Chance, eine qualitativ hochwertige KI zu entwickeln, ist also eher hoch, und gleichzeitig ist die potentielle Arbeitserleichterung ebenfalls hoch. Zudem kann das Ergebnis manuell nachkorrigiert werden, womit im Einzelfall keine allzu negative Konsequenz droht, wenn die KI einige wenige Fehler macht (solange der angestrebte Recall erreicht wird).

2. Lügendetektor

Auch beim Szenario des Lügendetektors stellt sich zunächst die Frage nach der Datenart: Soll nur das Video ausgewertet werden oder zusätzlich auch die Tonspur? Für welche Sprache soll die KI trainiert werden (da sie dann auch nur für diese Sprache eingesetzt werden kann)? In welchem Kulturkreis leben die Personen, deren Aussagen auf Lüge oder Wahrheit untersucht werden sollen? etc.

Als nächstes stellt sich die Frage, wie hier realistische Daten zu Trainingszwecken erhoben werden können. Hier stoßen wir auf ein großes Fragezeichen: Wenn die KI am Ende eingesetzt werden soll, um in einem Gerichtsverfahren lügende Personen zu identifizieren, dann müssen die Trainingsdaten ebenfalls Personen beinhalten, die in dieser Situation waren. Denn es ist natürlich etwas ganz anderes, ob eine Person vor Gericht ist und eine Aussage macht, bei der es potenziell um eine lebenslange Freiheitsstrafe geht, oder ein*e Schauspieler*in so tun soll, als würde sie gerade lügen. Diese Videosequenzen – so man sie überhaupt erheben kann – müssen dann mit den korrekten Labels ausgestattet werden, das heißt irgendjemand muss sicher sagen können, ob diese Person gelogen hat oder nicht. Denn die KI soll daraus lernen und wenn Daten die Wahrheit nicht abbilden, kann die KI auch keinen wahren Zusammenhang lernen – „garbage in – garbage out". Doch wer soll beurteilen können, ob die Aussage eine Lüge darstellt oder nicht?

Abschließend stellt sich die Frage, was in Produktion mit der Vorhersage der KI gemacht wird: Ein beispielhaftes Ergebnis wäre ja, dass der Person eine vorhergesagte „Lüge-Wahrscheinlichkeit" von x % zuge-

wiesen wird. Diese Wahrscheinlichkeit kann unter Umständen eine Entscheidungshilfe sein – es bleibt aber die Frage, wie genau sie im Gerichtsprozess weiterverwendet werden soll.

Zusammenfassend scheint dies bei erster Betrachtung kein vielversprechender Anwendungsfall für eine KI zu sein, da eine eher nicht repetitive Aufgabe betroffen ist und eine Einzelfallentscheidung mit einem sehr hohen Impact für eine einzelne Person verbunden sein kann.

Lügendetektoren stellen dagegen eher keinen Anwendungsfall für KI dar

3. Hate Speech

Als letztes Beispiel betrachten wir die Entdeckung von Hate Speech in den Sozialen Medien. Wieder muss zunächst klar definiert werden, was genau entdeckt werden soll, hier also, was genau Hate Speech ist. Zudem muss die zu untersuchende Sprache festgelegt werden sowie die Art der zu untersuchenden Texte. Beispielsweise gibt es auf unterschiedlichen Plattformen unterschiedliche Zeichenbegrenzungen, was sich wiederum auf die Art der Texte auswirken kann.

Die reine Datenakquise dürfte sich hier zunächst unproblematisch gestalten: Oft bieten Plattformen dedizierte Schnittstellen (sog. APIs) an, um auf Inhalte zuzugreifen. Auch hier benötigen wir zusätzlich zu Beispielen von Hate Speech Negativbeispiele, also Textausschnitte, die keine Hate Speech enthalten, sowie ausreichend viele Grenzfälle. Grenzfälle können etwa Beispiele sein, die zwar Abwertungen enthalten, aber trotzdem nicht als Beleidigung zählen. Alle diese Textausschnitte müssen wiederum von Menschen gelabelt werden – also in „Hate Speech“ und „keine Hate Speech“ unterteilt werden.

Vielversprechender ist der Einsatz von KI zur Entdeckung von Hate Speech

Als Modellklasse für das Training des Modells bieten sich hier Verfahren aus dem Bereich „Natural Language Processing“ an; oftmals sind das Methoden des Deep Learning.

Sollte nun bei der Evaluation mehr Wert auf Precision oder Recall gelegt werden? Das kann von der Perspektive abhängen: Wenn eine bestimmte Social-Media-Plattform sich selbst damit rühmen will, „frei von Hate Speech zu sein“, dann will sie jede einzelne Stecknadel im Heuhaufen finden – jede Beleidigung herausfiltern –, also einen hohen Recall erreichen. Aus Sicht der Strafverfolgung (einmal abgesehen davon, dass Beleidigungen in der Regel Antragsdelikte sind, dies also möglicherweise kein praxisrelevantes Szenario ist) könnte man hingegen argumentieren, dass jede identifizierte „Beleidigung“ auch verfolgt werden

Recall oder Precision – das hängt von der Perspektive ab

können soll. Hier kann also eine hohe Precision wichtiger sein, um die Ressourcen auf tatsächlich relevante Fälle fokussieren zu können.

Zusammenfassend eignet sich dieses Szenario – je nach Blickwinkel – gut für den Einsatz einer KI, da es sich um eine große Menge von im Mittel eher einfachen Entscheidungen handelt und eine Fehlentscheidung der KI keine gravierende Konsequenz für ein Individuum nach sich zieht.

V. Weitere Aspekte von ML

Zur Abrundung werden nun noch einige weitere wichtige Aspekte von ML behandelt; eine tiefere Auseinandersetzung mit den Begriffen würde den Rahmen dieses Beitrags allerdings sprengen.

1. Andere Arten von ML

Neben dem überwachten maschinellen Lernen (Supervised ML), mit dem wir uns bis hierher beschäftigt haben, gibt es auch den Zweig des unüberwachten maschinellen Lernens (Unsupervised ML). Hier enthält der Datensatz keine Zielvariable, also kein Target. Stattdessen wird versucht, Muster und Zusammenhänge in den Features zu finden. Eine weitere Richtung ist das Reinforcement Learning, das oft verwendet wird, um beispielsweise eine KI zu trainieren, die lernen soll, ein Computerspiel zu beherrschen.

2. Problemstellungen

Eine Problemstellung in ML ist die Quantifizierung von Unsicherheit. Zusätzlich zu der binären Entscheidung einer Klassifikation (z.B. Hate Speech ja/nein), soll hier der Grad der Unsicherheit quantifiziert werden. Dies ist in der aktuellen Forschung ein sehr relevantes und intensiv bearbeitetes Thema, da die reine Klassifikationsgüte oft zwar sehr hoch ist, die Quantifizierung der Unsicherheit aber noch nicht zufriedenstellend gelöst ist.

Auch ist wahrscheinlich bekannt, dass „Korrelation keine Kausalität" ist beziehungsweise dass ein Zusammenhang und ein kausaler Effekt unterschiedliche Konzepte sind. Typischerweise werden per ML nur Zusammenhänge gelernt. Auf dem hochaktuellen Gebiet der Causal Inference werden jedoch zunehmend Überlegungen dazu angestellt, wie

aus der Kombination von Daten und fachlicher Expertise Wissen über kausale Wirkungsketten abgeleitet werden kann.

Im Bereich der ethischen Fragen ist u.a. die Fairness ein vieldiskutiertes Thema und die Frage, ob und wie ML-Modelle unfair sein oder unfaire Behandlungen induzieren können, hochaktuell.[23] Außerdem stellt sich wie bei jeder fortgeschrittenen Technologie die Frage, ob man alles, was man tun *kann*, auch tun *soll*, und wie viele und welche Arten von Entscheidungen man automatisieren will.

2. Mythen und Halbwahrheiten

Im Übrigen ist es ein zentraler Aspekt der Arbeit mit ML, die tatsächlichen Möglichkeiten von Mythen und Halbwahrheiten abzugrenzen, von denen oft zu hören und zu lesen ist.

a) „KI ist selbstlernend"

Diese Aussage vermittelt den Eindruck einer höheren Macht, die „von alleine" Neues lernt und uns irgendwann überflügeln wird. Wie wir jedoch gesehen haben, wird innerhalb des Lernprozesses versucht, ein Zusammenhang zwischen Target y und Features x zu lernen, also eine Funktion f(x). Wenn diese Funktion gelernt wurde, ist der Lernprozess allerdings abgeschlossen – die KI lernt nicht „von alleine" auf magische Weise weiter. Natürlich kann der Lernprozess mit neuen Trainingsdaten neu gestartet werden. Wenn dieser Lernprozess sogar mehrmals am Tag neu gestartet wird, ist es im Ergebnis tatsächlich so, dass das benutzte ML-Modell immer besser werden kann; aber es ist nicht so, dass die KI von sich aus etwas lernt, sondern es ist immer noch ein Mensch, der eine Software programmiert hat, die diesen Lernprozess regelmäßig neu anstößt.

> Eine KI lernt nicht von sich aus immer weiter, sondern es ist ein Mensch, der die Software programmiert hat, die diesen Lernprozess regelmäßig neu anstößt

b) „KI ist eine unerklärbare Black Box"

In gewisser Weise gibt es diesen Charakter der Black Box, aber ganz unerklärbar ist eine KI bzw. ein ML-Modell nicht. Die Bereiche des Interpretierbaren maschinellen Lernens (IML) bzw. der Explainable Artificial Intelligence (XAI) beschäftigen sich intensiv damit, ML-Modelle erklärbarer zu machen. Zusätzlich sei hier angemerkt, dass auch

[23] Einen ausführlichen Überblick über das Thema Fairness in ML gibt das Buch von *Barocas/Hardt/Narayanan*, Fairness and Machine Learning, 2019.

menschliche Entscheidungen zu einem gewissen Grad eine Black Box sein können.

c) „KI ist unbrauchbar, weil sie nicht 100 % Genauigkeit erreicht“

Es ist völlig korrekt, dass eine KI in der Praxis nicht zu 100 % genau sein wird – genauso wenig wie ein Mensch nie Fehler macht. Die entscheidende Frage ist daher eher: Ist die Fehlerrate für den avisierten Einsatz akzeptabel oder nicht?

VI. Fazit

KI ist keine magische Wundermaschine, kann aber für die richtigen Fragestellungen und bei angemessener Verwendung gewinnbringend sein. Vielversprechende Fragestellungen sind repetitive und klar beschreibbare Probleme; sobald sehr ähnliche Dinge sehr oft getan werden müssen, kann man darüber nachdenken, ein ML-Modell dafür zu trainieren. Angemessene Verwendung bedeutet: Auf der einen Seite braucht es technisches Verständnis, in diesem Zusammenhang auch teilweise mit „statistical literacy“ bezeichnet, also Fähigkeiten aus dem Bereich Statistik, Mathematik und Informatik. Auf der anderen Seite ist die Fachkenntnis der Anwender*innen entscheidend. Jeder erfolgreiche ML-Use Case wird immer aus einer Kooperation von technischer Seite und Anwenderseite entstehen.

KI ist keine magische Wundermaschine, kann aber bei richtiger Verwendung gewinnbringend sein

Literatur

Angwin, Julia / Larson, Jeff / Mattu, Surya / Kirchner, Lauren: Machine Bias, Propublica, 25.5.2015, abrufbar unter https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

Application Security Series: Top 10 Failures of AI, 02.06.2020, abrufbar unter https://www.immuniweb.com/blog/top-10-failures-of-ai.html.

Barocas, Solon / Hardt, Moritz / Narayanan, Arvind: Fairness and Machine Learning. Limitations and Opportunities, 2019, abrufbar unter https://fairmlbook.org/.

Beuth, Patrick: Twitter-Nutzer machen Chatbot zur Rassistin, Die Zeit, 24.03.2016, abrufbar unter https://www.zeit.de/digital/internet/2016-03/microsoft-tay-chatbot-twitter-rassistisch.

Boser, Bernhard E./Guyon, Isabelle M./Vapnik, Vladimir N: A training algorithm for optimal margin classifiers, in: Proceedings of the 5th Annual ACM Workshop on Computational Learning Theory, Association for Computing Machinery, S. 144–152, New York 1992.

Breiman, Leo / Friedman, Jerome H. / Olshen, Jerome H. / Stone, Charles J.: Classification And Regression Trees, New York 1984.

Breiman, Leo: Random Forests, Machine Learning 2001 (45), S. 5–32. 2001, abrufbar unter https://link.springer.com/article/10.1023/A:1010933404324.

Chen, Tianqi / Guestrin, Carlos: XGBoost: A Scalable Tree Boosting System, Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Association for Computing Machinery 2016, S. 785–794, abrufbar unter https://dl.acm.org/doi/10.1145/2939672.2939785.

Cellan-Jones, Rory: Stephen Hawking warns artificial intelligence could end mankind, BBC 02.12.2014, abrufbar unter https://www.bbc.com/news/technology-30290540#:~:text=Prof%20Stephen%20Hawking%2C%20one%20of,end%20of%20the%20human%20race.%22.

Europäisches Parlament: Was ist künstliche Intelligenz und wie wird sie genutzt?, 29.03.2021, abrufbar unter https://www.europarl.europa.eu/news/de/headlines/society/20200827STO85804/was-ist-kunstliche-intelligenz-und-wie-wird-sie-genutzt.

Fulterer, Ruth: Warum automatische Übersetzer so gut funktionieren, NZZ, 29.01.2022, abrufbar unter https://www.nzz.ch/technologie/wie-kuenstliche-intelligenz-die-sprachgrenzen-verschwinden-laesst-ld.1666356.

Goodfellow, Ian / Bengio, Yoshua / Courvilleet, Aaron: Deep Learning, Cambridge 2016, abrufbar unter: https://www.deeplearningbook.org/.

Hawkins, Andrew J.: Uber is at fault for fatal self-driving crash, but it's not alone, The Verge, 19.11.2019, abrufbar unter https://www.theverge.com/2019/11/19/20972584/uber-fault-self-driving-crash-ntsb-probable-cause.

James, Gareth / Witten, Daniela / Hastie, Travor / Tibshirani, Robert: An Introduction to Statistical Learning – with Applications in R, Berlin 2021, abrufbar unter: https://link.springer.com/book/10.1007/978-1-0716-1418-1.

Jiru, Josef: Autonomous Driving, Fraunhofer Institute for Cognitive Systems IKS, abrufbar unter https://www.iks.fraunhofer.de/en/topics/autonomous-driving.html.

Kersting, Kristian / Lampert, Christoph / Rothkopf, Constantin: Wie Maschinen lernen – Künstliche Intelligenz verständlich erklärt. Berlin 2019, abrufbar unter https://link.springer.com/book/10.1007/978-3-658-26763-6.

Lovell, Tammy: BioNTech and InstaDeep join forces to predict high-risk COVID variants, healthcareitnews.com, 18.1.2022, abrufbar unter https://www.healthcareitnews.com/news/emea/biontech-and-instadeep-join-forces-predict-high-risk-covid-variants.

Metz, Cade: Who Is Making Sure the A.A. Machines Aren't Racist? New York Times, 15.3.2021, https://www.nytimes.com/2021/03/15/technology/artificial-intelligence-google-bias.html

Reuter, Markus: China testet Gefühlserkennung an uigurischer Minderheit, netzpolitik.org, 27.05.2021, abrufbar unter https://netzpolitik.org/2021/kuenstliche-intelligenz-china-testet-gefuehlserkennung-an-uigurischer-minderheit/.

Schulz, Elena: DeepMind-KI schlägt Starcraft-Profis – Menschliche Spieler nahezu chancenlos, gamestar.de 27.01.2019, abrufbar unter https://www.gamestar.de/artikel/deepmind-ki-schlaegt-starcraft-profis-menschliche-spieler-nahezu-chancenlos,3339818.html.

Seif, George: An Easy Introduction to Machine Learning Recommender Systems, KDnuggets, 04.09.2019, abrufbar unter

https://www.kdnuggets.com/2019/09/machine-learning-recommender-systems.html.

Siemens-Stiftung, Medienportal für den MINT-Unterricht: Künstliche Intelligenz – Praxisbeispiel: Gesichtserkennung, 2019, abrufbar unter https://medienportal.siemens-stiftung.org/download/112298.

Urbanek, Margarethe: Künstliche Intelligenz versus Ärzte. Wer Brustkrebs besser diagnostiziert, Ärztezeitung, abrufbar unter https://www.aerztezeitung.de/Wirtschaft/Wer-Brustkrebs-besser-diagnostiziert-405409.html.

IMPRESSIONEN AUS DER DISKUSSION…

„Was sind eigentlich neuronale Netze?“

„Neuronale Netze sind eine Art von Modell maschinellen Lernens. Was bei diesen neuronalen Netzen passiert, ist im Endeffekt nichts anderes, als dass wieder genauso eine Funktion f(x) gelernt werden soll, also der Zusammenhang von Features x und Target y. Der Begriff "neuronales Netz" kommt daher, dass man sich das ML-Modell als ein solches Netz vorstellen kann: Wir haben z.B. drei Features, unter anderem Alter und Vorstrafen. Was jetzt z.B. passiert ist, dass diese Features gewichtet und dann aufsummiert werden. Das Ergebnis ist also einfach eine bestimmte Funktion f(x). Neuronales Netz heißt es deswegen, weil man das vergleichbar einem solchen Netz visualisieren kann. Im Endeffekt würde ich sagen, dass das ein guter Marketingbegriff ist. Offensichtlich ein sehr guter Marketingbegriff, aber eigentlich geht es nur darum, dass ich eine Funktion finde, die den Zusammenhang zwischen Features und Zielvariable beschreibt. Diese Netze können natürlich noch komplexer werden als in diesem Beispiel hier.“

„Denken Sie, dass im Strafrecht Juristen langfristig zum großen Teil durch KI ersetzt werden können?“

„Ich kann mir das nicht vorstellen. Jetzt weiß ich natürlich nicht gut genug darüber, was genau eine Jurist*in in der Praxis tatsächlich tun muss, um zu wissen, was man davon vielleicht auch durch eine Maschine ersetzen könnte. Ich würde trotzdem sagen: Ein Gericht wird man niemals durch eine Maschine ersetzen wollen. Vielleicht kann man Dinge unterstützen, Entscheidungshilfen geben, wie etwa hinsichtlich einer Rückfälligkeitsprognose. Ich glaube, dass, wenn man überhaupt unterstützen kann, man dabei helfen kann, dass Staatsanwaltschaften und Gerichte effizienter arbeiten können. Man hört ja immer wieder, dass Gerichte, Staatsanwaltschaften und Polizei überlastet sind. Wenn Dinge, die nicht unbedingt ein Volljurist, eine Volljuristin tun muss, durch eine Maschine ersetzt werden, dann können sich diese Volljurist*innen, die es immer noch geben wird, vielleicht auf die wichtigeren Dinge konzentrieren. Das wäre jetzt meine Prognose, weil es bei den Rechtswissenschaften doch auch sehr viel um Einzelschicksale geht. Da kann ich mir nicht vorstellen, dass man das in absehbarer Zeit durch Maschinen ersetzen kann – oder will.“

„Könnten Sie nochmal den Unterschied zwischen Supervised und Unsupervised bzw. Reinforcement Learning erklären?“

„Ohne jetzt zu sehr ins Detail zu gehen: Im Unsupervised Learning ist die Ausgangslage, dass kein Target y in den Daten enthalten ist, sondern nur Features x. Mit Unsupervised Learning wird versucht zu lernen, diese Punkte in Klassen zu gruppieren, ohne dass aber die wahren Klassen bekannt wären.

Beim Reinforcement Learning soll über positive und negative Incentives gelernt werden: Wenn also eine Maschine lernen soll, Schach zu spielen, dann lässt man die Maschine zufällig Strategien entwickeln und sagt ihr am Ende, ob sie gewonnen hat oder nicht; auf diese Weise können zielführendere Strategien positiv bewertet werden. Basierend darauf ist es dann auch wieder Supervised Learning, weil das Ziel das Gewinnen ist, aber ich lasse ihr die Möglichkeit, selber Strategien zu finden.“

„Sehen Sie Chancen in der Verwendung von maschinellem Lernen bei politischen Wahlkämpfen? Gibt es bereits Bestrebungen einzelner Parteien, das zu nutzen?“

„Bei den letzten US-Wahlen ist wohl genau das passiert – dass maschinelles Lernen eingesetzt wurde. Bestimmte Gruppen von potenziellen Wähler*innen wurden gesucht, die man vielleicht noch beeinflussen könnte, und diesen wurden dann Informationen gegeben, die sie in eine bestimmte Richtung beeinflussen sollten. Für Deutschland habe ich so etwas noch nicht gehört, aber es muss natürlich auch nicht immer manipulativ sein. Wenn man will, kann man sagen, jede Wahlforschung ist irgendwie maschinelles Lernen, das ist klassische Statistik, die Übergänge sind fließend – maschinelles Lernen kann man heutzutage ein bisschen besser verkaufen als Statistik. Statistik ist irgendwie langweilig, Machine Learning ist cool, also machen wir jetzt halt Wahlforschung mit Machine Learning!“

DOI: 10.5282/ubm/epub.92172
https://doi.org/10.5282/ubm/epub.92172
München 2022