TAGUNGSBERICHTE

Erlanger Cybercrime Tag 2023: Open Source Intelligence in der Strafverfolgung

von Tabea Seum und
Prof. Dr. Christian Rückert[*]

Abstract
Der Tagungsbericht enthält sprachlich bereinigte und gekürzte Zusammenfassungen der Transkriptionen der Vorträge und Diskussionsbeiträge. Der Vortragsstil der einzelnen Beiträge wurde überwiegend beibehalten (soweit nicht aus Platzgründen gekürzt wurde). Dementsprechend wurde generell auch auf Fußnoten verzichtet.

I. Einleitung

Nach einigen Jahren hieß es nun beim achten Erlanger Cybercrime Tag „back to the roots". Die Tagung wurde – wie in den Anfangsjahren – zum einen im Frühjahr abgehalten und zum anderen konnten die Teilnehmer:innen endlich wieder am ursprünglichen Tagungsort, im Wassersaal der Orangerie, begrüßt werden. Um jedoch über die Plätze der Orangerie hinaus noch Interessierte erreichen zu können, entschied man sich für eine hybride Tagung. Dadurch konnten insgesamt fast 180 Teilnehmer:innen den Vorträgen folgen und an den sich jeweils anschließenden Q&A-Sessions teilnehmen. Das Publikum war, wie auch in den vorherigen Jahren, bunt gemischt und setzte sich aus Vertretern der Wissenschaft, der Strafrechtspraxis sowohl aus Justiz als auch der Anwaltschaft, Fachvertreter:innen und auch Studierenden zusammen. *Prof. Dr. Christoph Safferling* und sein ICLU-Team freuten sich auch dieses Mal, dass die unterschiedlichen Perspektiven und die Interdisziplinarität der Vorträge und Teilnehmer zu einem bereichernden Austausch beitrugen.

Der diesjährige ECCT beschäftigte sich mit sog. OSINT-Ermittlungen im Strafverfahren. Dabei wurden unterschiedliche – teilweise sehr grundlegende, teilweise sehr tiefgehende – Fragestellungen thematisiert. Was ist „Open Source Intelligence" (kurz: OSINT)? Welche rechtlichen Probleme und Herausforderungen können sich ergeben? Wie nutzen die Strafverfolgungsbehörden die Möglichkeiten der Ermittlungsmaßnahme im Alltag? Welche rechtlichen und tatsächlichen Grenzen müssen beachtet werden? Welche Probleme und Möglichkeiten ergeben sich aus Strafverteidigersicht? Und wie kommt OSINT im internationalen Kontext und durch die Verwendung von Menschenrechtsorganisationen zur Anwendung? Diese und viele weitere Fragen wurden anschaulich und intensiv mit den referierenden Expert:innen *Prof. Dr. Christian Rückert* (Universität Bayreuth), Kriminalhauptkommissar *Andreas Korn* (BayLKA), Oberstaatsanwalt *Dr. Nino Goldbeck* (ZCB), Rechtsanwältin *Diana Nadeborn* (Tsambikakis & Partner) und Rechtsanwalt *Kai Kempgens* (damals kpw, heute Eisenberg König Schork Kempgens), *Prof.in Dr. Katrin Kinzelbach* (FAU Erlangen-Nürnberg) diskutiert. Eröffnet wurde die Tagung mit den Begrüßungsworten des Präsidenten der FAU Erlangen-Nürnberg, *Prof. Dr. Joachim Hornegger* und des stellvertretenden Sprechers des Graduiertenkollegs „Cybercrime und Forensische Informatik" der FAU und Inhaber des Lehrstuhls für Strafrecht, Strafprozessrecht und Rechtsphilosophie, *Prof. Dr. Hans Kudlich*.

II. OSINT in der StPO – Ermittlungen ohne Rechtsgrundlage? von Prof. Dr. Christian Rückert (Universität Bayreuth)

Sowohl die Einleitungs- als auch die ersten Vortragsworte wurden von *Prof. Rückert* gesprochen, der die Veranstaltung selbst jahrelang mitorganisiert und -gestaltet hatte. Anlehnend an seine Habilitationsschrift[1], veranschaulichte er den Veranstaltungsinteressierten den Begriff OSINT und die Rolle dieser Technik bei den Strafverfolgungsbehörden. Daran anknüpfend, führte er die rechtlichen Probleme aus, die sich bei der Durchführung von OSINT-Maßnahmen durch die Polizei oder Staatsanwaltschaft hinsichtlich möglicher Grundrechtseingriffe, einer notwendigen Rechtsgrundlage in der StPO und des europäischen Datenschutzrechts ergeben können.

1. Der Begriff Open Source Intelligence

Open Source Intelligence ist ein Begriff aus der Nachrichtendienstwelt, welcher früher Medien, wie Zeitungen oder das Radio, umfasst hatte, mittlerweile in der Regel jedoch die Erhebung von Daten aus dem Internet meint. Im Rahmen von Open Source Intelligence werden Informationen aus öffentlich zugänglichen Quellen gesammelt und ausgewertet, um Erkenntnisse zu gewinnen. Das bedeutet, dass solche Maßnahmen zwar auch ein bloßes Googlen umfassen, jedoch weit darüber hinausgehen können. Von der Verwendung von Google angefangen, über sogenannte Web-Crawler bis hin zu automatisierten Suchprogrammen, die sich beispielsweise ein Gesamtbild eines

* *Tabea Seum* ist Wissenschaftliche Mitarbeiterin am Lehrstuhl von *Prof. Dr. Christoph Safferling* an der Friedrich-Alexander-Universität Erlangen-Nürnberg, *Prof. Dr. Christian Rückert* ist Inhaber des Lehrstuhls für Strafrecht, Strafprozessrecht und IT-Strafrecht an der Universität Bayreuth.

[1] *Rückert,* Digitale Daten als Beweismittel im Strafverfahren, 2023.

Darknet Marktplatzes schaffen, können jegliche Handlungen dabei sein. Durch die Automatisierung und Verwendung von KI-Tools ist vor allem mit der Verknüpfung weiterer Maßnahmen (z.B. Gesichtserkennungssoftwares zur Identifizierung) eine Masse der Datengewinnung möglich, die im Hinblick auf das Datenschutzrecht bedenklich erscheint. Sämtliche denkbare OSINT-Maßnahmen wurden dabei anhand von Beispielsfällen erläutert, die in diesem Beitrag aufgrund von notwendigen Kürzungen nicht dargestellt werden können.

2. Einordnung nach deutschem Verfassungs- und Strafprozessrecht

Nach der Definition und Begrenzung des OSINT-Begriffs und der Handlungsvielfalt wurde sodann ein schärferer Blick auf die nationale rechtliche Lage geworfen. Dabei ist festzuhalten, dass es keine konkrete Norm gibt, die OSINT-Maßnahmen regelt. Vielmehr bedürfen die Maßnahmen, soweit sie in Grundrechte eingreifen, und je nachdem wie intensiv sie sind, einer neuen und verfassungsgemäßen Rechtsgrundlage.

a) Vorliegen eines Grundrechtseingriffs

OSINT-Maßnahmen greifen in das Recht auf informationelle Selbstbestimmung als Teil des Allgemeinen Persönlichkeitsrechts ein. Dabei stellt sich die grundlegende Frage: Handelt es sich um einen Eingriff in das Grundrecht, wenn die Daten, um die es geht, öffentlich zugänglich sind? Zur Beantwortung dieser Frage unterscheidet das *BVerfG* in seiner Rechtsprechung zwischen der automatisierten Erhebung von Daten, die immer einen Eingriff darstellt, und manuell erhobenen Daten.[2] Bei Letzterem befinden sich die Strafverfolgungsbehörden in einem Bereich, in welchem sich ein normaler Bürger mit seinen Handlungen auch bewegen würde. Weiterhin muss man sich fragen, ob nicht durch das eigene Zugänglichmachen der Daten etwas Vergleichbares wie eine Einwilligung oder gar ein Verzicht auf das Grundrecht vorliegen kann. Dem steht jedoch der Inhalt des Rechts auf informationelle Selbstbestimmung entgegen. Das Recht schützt die Entscheidungsfreiheit darüber, wann, wie, wo und wozu persönliche Daten verwendet werden. Beim Einstellen von Bildern, Beiträgen, Videos usw. auf Social Media Plattformen wird vom Willen gerade nicht umfasst, dass Dritte die Daten und Informationen für Recherchen und Ermittlungen verwenden. Soziale Netzwerke haben die Funktion der Vernetzung von Menschen und sind kein Produkt staatlicher Behörden (wenngleich diese sie auch zu ihrem Vorteil nutzen können und wollen). Zusätzlich setzt das Recht auf informationelle Selbstbestimmung voraus, dass es sich um personenbezogene Daten handeln muss, was aber in den allermeisten Fällen anzunehmen ist. Somit lässt sich abschließend feststellen, dass es sich bei OSINT-Maßnahmen zwar nur um Googlen handeln kann, aber wenn der Strafverfolger googelt, es trotzdem als Eingriff in das Recht auf informationelle Selbstbestimmung einzuordnen ist.

b) Bestimmung der Eingriffsintensität

Grundsätzlich kommt die Ermittlungsgeneralklausel §§ 161, 163 StPO als Rechtsgrundlage in Betracht, die nach der Reform auch den Begriff der Datenerhebung in ihren Wortlaut aufgenommen hat. Aus dem Wesentlichkeitsvorbehalt ergibt sich jedoch, dass nur ein geringfügiger Eingriff durch die Generalklausel umfasst sein kann. Wie bestimmt man aber die Eingriffstiefe bei OSINT-Maßnahmen? Diese Frage wurde anhand einer vom Referenten entwickelten Kategorisierung beantwortet. Besprochen wurden Faktoren wie die Stärke des Personenbezugs, die Sphäre, aus der die Daten stammen (Sozial-, Privat, Intimsphäre bzw. Kernbereich) die Informationsdichte der Daten, die Heimlichkeit der Maßnahme, die Öffentlichkeit der Daten, inklusive der Frage, ob die Daten vom Betroffenen selbst öffentlich gemacht worden sind, die Streubreite und Automatisierung der jeweiligen OSINT-Methode. Nach Abwägung dieser Faktoren ergibt sich, dass sich die Heimlichkeit der Maßnahme als intensitätssteigernder Faktor und die öffentliche Zugänglichkeit der Daten als intensitätssenkender Faktor häufig bei OSINT-Maßnahmen ausgleichen können und sich die Schwere des Eingriffs sodann maßgeblich an der Streubreite bzw. Automatisierung messen lassen muss. Aufgrund der Vielfalt an denkbaren OSINT-Maßnahmen kann die Eingriffstiefe dabei nicht pauschal für alle OSINT-Methoden bestimmt werden. Vielmehr müssen die Strafverfolgungsbehörden eine Einzelfallabwägung anhand der o.g. Kriterien durchführen.

c) Gibt es eine Rechtsgrundlage für OSINT in der StPO?

Der Rückgriff auf die Generalklausel ist nur notwendig und möglich, wenn es keine speziellere Rechtsgrundlage gibt. Bei einem Blick in die StPO lässt sich jedoch keine passende Vorschrift finden. Die Norm zur Regulierung der Rasterfahndung § 98a StPO wurde gerade für die Erhebung nichtöffentlicher Daten geschaffen und unterscheidet sich somit grundlegend von OSINT-Ermittlungen. § 98c StPO, der den justiziellen maschinellen Datenabgleich umfasst, regelt den Abgleich von Daten, die bereits erhoben wurden, nicht jedoch die Erhebung von Daten. Außerdem stößt § 98c StPO an seine Grenzen, wenn zum maschinellen Datenabgleich moderne Methoden des Data Mining und der künstlichen Intelligenz eingesetzt werden, weil ein solcher Einsatz bei Schaffung des voraussetzungsarmen § 98c StPO nicht bedacht worden ist. Auch auf die §§ 100a ff. oder 163a ff. StPO kann nicht zurückgegriffen werden, da es sich dabei um sehr enge Spezialvorschriften für völlig andere Ermittlungsmethoden handelt. Ein Rückgriff auf die Generalklauseln der §§ 161, 163 StPO ist damit notwendig.

Als Zwischenbilanz lässt sich festhalten, dass für eine rein manuelle OSINT-Recherche (wie etwa eine händisch durchgeführte Google-Recherche) die Ermittlungsklausel ausreichend sein wird, da man hier in der Regel keinen schweren Grundrechtseingriff annehmen kann. Bei allem,

[2] *BVerfG*, Urt. v. 16.2.2023 – 1 BvR 1547/19; 1 BvR 2634/29.

was darüber hinausgeht, muss im Einzelfall anhand der o.g. Eingriffsschwerekriterien geprüft werden, ob tatsächlich noch ein „geringfügiger" Grundrechtseingriff vorliegt. Auf keinen Fall anwendbar scheint die Norm auf vollständig automatisierte OSINT-Recherchen mit großer Streubreite, wie etwa beim Einsatz von Web-Crawlern mit anschließender automatisierter – ggf. sogar KI-gestützter – Massendatenauswertung. Dies ergibt sich aus einer jüngeren Entscheidung des *BVerfG* aus dem Bereich des Data-Mining, aus der hervorgeht, dass bei einer Auswertung von Massendaten durch Techniken wie Machine Learning und KI der Grundrechtseingriff zu schwer ist, um solche Techniken auf die Ermittlungsgeneralklausel (und auch § 98c StPO) zu stützen.[3]

3. Datenschutzrecht und europarechtlicher Einfluss

Abgerundet wurde der Vortrag durch Bezugnahmen auf das strafprozessuale Datenschutzrecht inklusive seiner europäischen Grundlagen in der Richtlinie 2016/680/EU. Die §§ 45 ff. BDSG, welche die Umsetzungsnormen der o.g. Richtlinie sind, sind über § 500 StPO (für Landesbehörden und -gerichte) sowie über § 1 Abs. 1 Nr. 1 BDSG (für Bundesbehörden und -gerichte) auch im Strafverfahrensrecht anwendbar. Da die Generalklausel – im Gegensatz zu den Spezialvorschriften – kaum Verfahrensregelungen oder Schutzmechanismen enthält, kommt das BDSG trotz des (außerdem aus Sicht des Referenten europarechtswidrigen) lex specialis-Vorbehalts des § 500 Abs. 2 Nr. 1 StPO zur vollen Anwendung bei OSINT-Maßnahmen. Das führt dazu, dass hier nicht nur die Rechtsprechung des *BVerfG* gilt, sondern aufgrund der Grundlage der §§ 45 ff. BDSG in der genannten europäischen Richtlinie und der aktuellen Rechtsprechung des *BVerfG* (Recht auf Vergessen I und II sowie Europäischer Haftbefehl III) auch die Entscheidungen des *EuGH* und des *EGMR* zu berücksichtigen sind. Wichtige Unterschiede zwischen nationalem und europäischem Recht können sich zum einen bei den Anforderungen an den Erforderlichkeitsbegriff ergeben, da dieser im Europarecht strenger ist als auch bei der Kategorisierung von sog. sensitiven Daten nach § 48 BDSG. Aber auch das Verbot von rein automatisierten Entscheidungen aus § 54 BDSG, muss beachtet werden.

a) Anforderungen an OSINT-Tools

Maßstab für die technische Gestaltung der eingesetzten OSINT-Tools ist dabei das Prinzip von Data Protection by Design and by Default, wie es sich aus § 71 BDSG ergibt. Demnach dürfen bei einer Automatisierung nicht pauschal jegliche Daten erhoben werden, sondern es bedarf einer Filterfunktion, um eine Vorratsdatenerhebung und -speicherung zu vermeiden. Weiterhin müsste eine Differenzierung im Rahmen der Personenkategorien (Zeuge, Schuldiger, Opfer, usw.) gem. § 72 BDSG erfolgen und zum anderen eine strenge Unterscheidung zwischen Tatsachen und persönlichen Einschätzungen nach § 73 BDSG. Zu persönlichen Einschätzungen gehört dabei nach Auffassung des Referenten alles, was nicht unzweifelhaft bewiesen ist und damit auch Erkenntnisse, die sich aus statistischen Datenverarbeitungsmethoden ergeben. Aus § 64 BDSG ergeben sich schließlich spezifische Anforderungen an die IT-Sicherheit der Datenverarbeitung durch Polizei und Justiz.

b) Benachrichtigungspflicht

Während für die in der StPO spezifisch geregelten heimlichen Ermittlungsmaßnahmen wie etwa die TKÜ jeweils Benachrichtigungspflichten gesetzlich vorgesehen sind (siehe z.B. § 101 Abs. 4 StPO), fehlt eine solche Benachrichtigungsvorschrift für heimliche Maßnahmen, die auf die Ermittlungsgeneralklausel gestützt werden. Nach § 47 Nr. 1 Var. 2 BDSG muss jedoch jede strafprozessuale Datenverarbeitung dem Grundsatz von „Treu und Glauben" entsprechen, was nach der maßgeblichen europarechtskonformen Auslegung auch eine Benachrichtigungspflicht bei heimlicher Datenverarbeitung umfasst. Daher hätte der Gesetzgeber nach der Auffassung des Referenten bei der Umsetzung der Richtliniennorm des Art. 4 Abs. 1 lit. a RL 2016/680/EU, welcher die Grundlage für § 47 Nr. 1 Var. 2 BDSG ist, auch eine allgemeine Benachrichtigungspflicht für heimliche Ermittlungsmaßnahmen auf Grundlage der Generalklauseln mitregeln müssen. Dies führt dazu, dass die Anwendung der Ermittlungsgeneralklausel für heimliche Ermittlungsmaßnahmen und damit auch heimlich durchgeführte OSINT-Ermittlungen europarechtswidrig ist. Ein vom Referenten beschriebener Ausweg könnte – bis zu einer entsprechenden Regelung durch den Gesetzgeber – eine analoge Anwendung von § 101 Abs. 4 StPO sein. Das kommt vor allem deshalb in Betracht, weil die europarechtskonforme Auslegung insbesondere auch Analogien umfasst bzw. ermöglicht und durch diese Analogie ein positiver Effekt für den betroffenen Grundrechtsträger eintreten würde.

4. Fazit

Es lässt sich festhalten, dass unter Open Source Intelligence eine Vielzahl an Maßnahme- und Handlungsmöglichkeiten fallen. Dabei greifen fast alle in das Recht auf informationelle Selbstbestimmung ein und bedürfen daher einer verfassungsgemäßen Rechtsgrundlage. Im Einzelfall ist wichtig, wie die Eingriffsintensität bewertet wird, wobei sich die Faktoren „heimliche Maßnahme" und „öffentlich zugängliche Daten" bei einer Abwägung neutralisieren könnten. Die Intensität wird sich dann eher durch Streubreite der Daten und eine mögliche Automatisierung ermitteln lassen. Da die StPO keine Spezialnorm für OSINT-Maßnahmen enthält, wird auf die Ermittlungsgeneralklausel zurückgegriffen, was jedoch allein bei tatsächlich nur „geringfügig" in die Grundrechte eingreifenden OSINT-Maßnahmen – wie etwa einfache manuelle Recherchen mit Suchmaschinen – möglich ist. Keinesfalls können die Generalklauseln den vollautomatisierten Einsatz von Web-Crawlern und Data Mining-Techniken rechtfertigen. Ferner müssen die § 345 ff. BDSG als Umsetzungsnormen der Richtlinie 2016/680/EU berücksichtigt werden. Besonders hervorzuheben ist dabei eine nach europäischem Recht notwendige, bislang in der StPO je-

[3] *BVerfG*, Urt. v. 16.2.2023 – 1 BvR 1547/19; 1 BvR 2634/29.

doch fehlende, ausdrückliche Pflicht zur Benachrichtigung bei der Datenverarbeitung im Rahmen von heimlichen OSINT-Maßnahmen, wobei es sich um ein Problem handelt, das über OSINT-Maßnahmen hinaus geht und derzeit über eine Analogie zu bewältigen ist.

5. Q&A – Session

In der sich anschließenden Q&A-Session wurde vertieft über die Grenzen von Sozial-, Privat- und Intimsphäre gesprochen, wobei Rechtsprechung und Literatur insoweit unterschiedliche Meinungen vertreten. Auch die Rolle von Beweisverwertungsverboten und eine etwaige Fernwirkung wurden diskutiert. *Prof. Rückert* konnte aufzeigen, dass OSINT-Maßnahmen, welche in sogenannten Vorermittlungen durchgeführt werden, nicht unter die StPO zu fassen sind, da insoweit in nahezu jeder Norm, aber vor allem von der Generalklausel ein Anfangsverdacht verlangt wird. Für Interessierte wurde auf die Stellungnahme des Ethikrates verwiesen[4] und auf § 32a AO, der die Finanzbehörden unter Umständen von einer Benachrichtigungspflicht befreit. Der Referent erläuterte, wieso nach seiner Ansicht §§ 100g und 100k StPO nach der gesetzgeberischen Konzeption und der verfassungsgerichtlichen Rechtsprechung eigentlich keine heimlichen Maßnahmen sein sollten, es in der Rechtspraxis aber *de facto* weiterhin sind, inwieweit man den Begriff „Heimlichkeit" abstufen kann und dass § 98a StPO auch nicht als angemessene Rechtsgrundlage in Betracht kommt, da sich die Norm auf bereits gespeicherte Daten auf einem Speichermedium bezieht und außerdem spezifisch auf nicht öffentlich zugängliche Daten zielt.

III. OSINT in der polizeilichen Ermittlung von Kriminalhauptkommissar Andreas Korn (Bayerisches Landeskriminalamt)

Nach dem dogmatischen Einstieg in die Thematik, konnte der nächste Referent den aufgezeigten und dargestellten Maßnahmen einen praktischen Bezug geben. *KHK Korn* gab einen offenen und interessanten Einblick in die Nutzung von OSINT-Maßnahmen im Rahmen der alltäglichen Polizeiarbeit.

1. Intelligence-Techniken

Open Source Intelligence gehört zur Familie der „Intelligence-Techniken". Daneben existieren weiteren Intelligence-Praktiken. Social Media Intelligence (SOCMINT) stellt dabei einen wichtigen Teilbereich von OSINT dar und umfasst alle Informationen, die aus Social Media Plattformen gewonnen werden können. Geospatial Intelligence (GEOINT) hingegen meint alle Geoinformationen, d.h. Daten und Informationen, die von Satelliten erzeugt werden. Mit Human Intelligence (HUMINT) ist die gewöhnliche Zeugenbefragung bzw. die Kontaktaufnahme mit Menschen im Rahmen einer Spionage gemeint.

Um die Relevanz und Nutzung von Geoinformationen greifbarer zu machen, folgt ein anschauliches Beispiel: Mit der Seite „Marine Traffic" kann man in Echtzeit verfolgen, welches Schiff sich auf welcher Position im Meer befindet. So konnte man unter anderem auch das im Suezkanal steckengebliebene Schiff *Ever Given* sehen. Aber nicht nur das blockierende Schiff, sondern auch alle Schiffe in der Nähe, die den Kanal nicht passieren konnten, konnte man verfolgen. Wieso sollte das interessant sein? Weil man sich anhand der einzelnen Schiffe ein Diagramm erstellen kann, welche Waren und Güter, aufgrund der Blockade und damit einhergehenden Verzögerungen, in den nächsten Monaten Probleme auf zum Beispiel dem europäischen Markt herbeiführen werden.

2. OSINT im polizeilichen Alltag

a) Allgemeines

In der Praxis sind Open Source Intelligence-Ergebnisse in der Regel nur der erste Schritt, um die Ermittlungen zu dynamisieren und nur selten das eigentliche Beweismittel. Neben OSINT verwendet die Polizei natürlich auch die klassischen Ermittlungsmaßnahmen: Spuren und Indizien wie die Forensik, daktyloskopische Spuren oder DNA, den Tatort, das Täterfahrzeug und Fingerspuren. Je nachdem an welche Beweismittel die Strafverfolgungsbehörden gelangt sind, wird entschieden, welche Ansätze und Indizien mit OSINT kombiniert und weiterverfolgt werden, um die Ermittlungen dadurch voranzubringen. Im Ermittlungsverfahren müssen nicht alle möglichen Social Media Portale genutzt werden, vielmehr wägen die Strafverfolgungsbehörden die relevanten und gewinnbringenden Sozialen Netzwerke von Einzelfall zu Einzelfall ab. OSINT-Ergebnisse sind in der Regel „nur" ein Hilfsmittel und führen nicht zur Verurteilung. Die Ergebnisse und Erkenntnisse müssen immer im Gesamtkontext betrachtet werden und aufgrund des Rechtsstaatsprinzip werden die Ergebnisse auf die Richtigkeit ihres Aussagegehalts überprüft.

b) OSINT-Quellen

Nach dem Auffinden erster Ergebnisse müssen die Daten selektiert und ausgewertet werden. Vor- und Nachname allein hilft den Strafverfolgungsbehörden für weitere Ermittlungen wenig, da im Internet keine Klarnamenpflicht besteht. Mit einer Telefonnummer hingegen können weitere Rückschlüsse auf die Identität einer Person gezogen werden. Die Länderkennung der Rufnummer kann bei einer Ortung helfen und bei Prepaid-Karten muss die Identität mittlerweile durch die Vorlage des Personalausweises bestätigt werden. Ein Hashwert wiederum kann durch ein Programm „auseinandergenommen" werden, um nützliche Informationen herauszulesen. Enthält die E-Mail-Adresse einen Nicknamen, kann dies ein Indiz für eine virtu-

[4] Deutscher Ethikrat, Stellungnahme „Mensch und Maschine – Herausforderungen durch Künstliche Intelligenz", 20.3.2024, online abrufbar unter: https://www.ethikrat.org/mitteilungen/mitteilungen/2023/ethikrat-kuenstliche-intelligenz-darf-menschliche-entfaltung-nicht-vermindern/?cookieLevel=not-set (zuletzt abgerufen am 6.5.2024).

elle Identität sein, die auch an anderen Stellen des World-WideWebs und Plattformen (im Darknet oder Verkaufsportalen wie Ebay oder Amazon) verwendet wird. Fotos, Bilder, Thumbnails, Text- und Chatnachrichtenauszüge lassen sich alle in den üblichen Plattformen finden (Facebook, Whatsapp, Threema, Telegram, Snapchat, Tiktok, Instagram). Interessant können aber auch Plattformen wie LinkedIn oder Xing sein, da die Daten dort meist der Wahrheit entsprechen. Ein oft genutztes Tool ist auch das TOR-Netzwerk, welches als dezentrales Netz und somit als Möglichkeit der Anonymisierung von Kriminellen genutzt werden kann. Zuletzt werden auch Überwachungskameras aus dem öffentlichen Raum für Ermittlungen herangezogen. Darunter existieren einige, die online aufrufbar sind.

3. Zukunftsprognose

Die Grundinteressen der Täter sind in der Regel auf Geld, Macht und sexuelle Überlegenheit zurückzuführen. Diese Bedürfnisse lassen sich auch auf die neuen möglichen virtuellen Welten wie das Web4 übertragen. Mit seinem eigenen Avatar durch die Welten via Virtual Reality oder Augmented Reality zu spazieren, bietet auch die Möglichkeit für Kriminalität und für ein „neues" Darknet. Weiterhin ist und bleibt der Bereich der Kryptowährungen – konkret des Bitcoins – relevant. Non-fungible Tokens sind mittlerweile mehrere Millionen Euro wert und im Bereich von ChatGPT und Künstlicher Intelligenz findet eine stetige Entwicklung mit neuen Möglichkeiten für Kriminelle statt. Dann wird man sich in Zukunft fragen müssen, wie man bei der Ermittlung eines virtuellen Diebstahls vorgehen muss.

4. Abschließendes Beispiel

Anhand eines Falles aus dem Alltag des Referenten erklärte dieser, wie das Landeskriminalamt die verschiedenen Tools und Techniken verwendet und welche Vor- und Nachteile sich ergeben. Im Fall wurde über eine Messenger App eine Amoklauf-Androhung ausgesprochen. Die Ankündigung allein ist schon strafbar, trotzdem wird die Polizei sowohl präventiv als auch repressiv tätig. Da der Schwerpunkt auf dem Schutz von Leib und Leben liegt, wird vorrangig das PAG angewendet und nur im Nachhinein auch auf Normen und Befugnisse aus der StPO zurückgegriffen. Zur Spurensuche und Findung von Lösungsansätzen hatten die Beamten am Anfang keine Telefonnummer oder E-Mail-Adresse, sondern nur Geo-Daten. Diese und auch IP-Adressen können jedoch verschleiert und gefälscht werden, zum Beispiel durch die Verwendung von Apps, die einen falschen Standort angeben. Über die Bilderrückwärtssuche von Google konnten jedoch weitere Indizien und mögliche Spuren durch die Meta-Daten des Bildes gefunden werden. Hilfreich waren vor allem die Chatnachrichten und deren Inhalte. Auch Chatinhalte können über Google gesucht und in anderen Plattformen gefunden werden. Der Nachrichteninhalt kann Informationen über die Identität, Lokalisation oder das Umfeld der Person geben. Durch die Kombination der verschiedenen Spuren und Indizien konnte der Täter am Ende ermittelt werden.

5. Q&A-Session

In der nachfolgenden Q&A-Session wurden vertieft Probleme zum Datenschutzrecht angesprochen. Insoweit bestehen gewisse Bedenken hinsichtlich der Nutzung von Google. Die Strafverfolgungsbehörden wissen das und können ihre Tätigkeiten durch die Nutzung von VPN Tunneln o.ä. verschleiern. Auch eine Nutzung von automatisierten Analysen im Bereich der sozialen Netzwerke findet statt, wobei die Ergebnisse überprüft werden müssen, um den Beweiswert sicherzustellen. Hinsichtlich KI generierter Bilder sieht *KHK Korn* derzeit keine Probleme, da der Polizei effektive Methoden zur Aufdeckung zur Verfügung stehen. Mit der stetigen Entwicklung der Technik könnte sich die Situation jedoch verändern, sodass ein denkbares Zukunftsszenario das Versehen der Bilder mit Hashwerten wäre.

IV. Open Source Material vor Gericht von Oberstaatsanwalt Dr. Nino Goldbeck (Zentralstelle Cybercrime Bayern)

Nach der Mittagspause übernahm *OStA Dr. Goldbeck* das Rednerpult. Er ist bei der Generalstaatsanwaltschaft in Bamberg mit seiner Arbeitsgruppe für die grenzüberschreitende Bekämpfung von Cybertrading verantwortlich und gewährt den Interessierten einen Einblick in seine alltäglichen Berührungspunkte mit OSINT-Maßnahmen. In seinem Vortrag möchte er das Publikum für den Einsatzbereich von Open Source Intelligence sensibilisieren.

1. Figur der Selbstbegebung

Den Vortrag von *Prof. Rückert* aufgreifend, führt der Referent Aspekte hinsichtlich der Eingriffstiefe von Grundrechten und dem diskutablen Punkt, wann man von öffentlich zugänglichen Daten sprechen kann, aus. Er verweist auf die von der Rechtsprechung entwickelte Figur der sog. Selbstbegebung.[5] Diese umfasst Personen, die entweder von vornherein in der Öffentlichkeit stehen oder im privaten Bereich gezielt versuchen, ihre Persönlichkeit oder ihren Erfolg publik zu machen. Im Presserecht findet sich dazu eine gefestigte Rechtsprechung, wonach man bei eigener „Aufgabe" seines Persönlichkeitsschutzes bis zu einem gewissen Punkt die Verwertung der Informationen durch andere hinnehmen muss. Dazu gehört auch die weitergehende Berichterstattung. Diese Werte könnte man in den strafrechtlichen Bereich übertragen oder im Rahmen einer Abwägung zumindest heranziehen.

2. OSINT in den einzelnen Verfahrensstadien

a) Ermittlungsverfahren

OSINT wird angewendet, wenn der Täter entweder noch unbekannt ist oder wenn eine Person im Tatverdacht steht und zur weiteren Untersuchung Erkenntnisse gewonnen werden müssen. Wie bereits angeklungen, werden durch OSINT-Ergebnisse meist nur Informationen gewonnen,

5 *BGH*, Urt. v. 12.6.2018 – VI ZR 284/17.

die dann zu einer weiteren Ermittlung und zu weiteren Indizien und Ansätzen führen. Die meiste Arbeit wird derzeit noch manuell durchgeführt, auch wenn es durchaus automatisierte Verfahren gibt, beispielsweise den Dark Web Monitor. Open Source Intelligence kann zwar auch bei Bagatelldelikten herangezogen werden, eine erhebliche Bedeutung kommt den Maßnahmen jedoch im Bereich der Schwerstkriminalität zu. Relevante Straftatbestände sind das Betreiben krimineller Handelsplattformen im Internet, die Bildung krimineller Vereinigungen, gewerbs- und bandenmäßiger Betrug, Geldwäsche, Computerbetrug und der gesamte Bereich der Kinderpornografie. Dabei handelt es sich um Katalogtaten i.S.d. § 100b StPO, sodass auch die Online-Durchsuchung möglich wäre. Zu einer effektiven Ermittlung der Strafverfolgungsbehörden ist es wichtig, soweit Grundrechtseingriffe durch OSINT-Maßnahmen vorliegen, dass diese in irgendeiner Form gerechtfertigt werden. Vor allem im Bereich internationaler Arbeit ist Open Source Intelligence unverzichtbar, da die Technik eine wichtige alternative Herangehensweise zur Erlangung von Informationen ist, wenn man auf kooperationsunwillige Staaten angewiesen ist. Typischerweise geht es dann um Fälle, in denen der Täter versucht, sich ins Ausland abzusetzen. Gleiches gilt aber auch im Bereich der Vermögenskriminalität, wenn es um die Frage der Identifizierung oder Lokalisierung von Vermögenswerten geht.

Aus Sicht des Referenten kommen als mögliche Lösungsansätze für eine etwaige Schwere des Grundrechtseingriffs Lösch-, Benachrichtigungs- und Meldepflichten in Betracht. Eine weitere aus der Praxis bekannte Methode wäre zudem das Führen eines Sonderheftes neben der Ermittlungsakte, welches die Daten mit Personenbezug enthält. Dadurch wäre sichergestellt, dass nur ein sehr kleiner Kreis an Verfahrensbeteiligten die sensiblen Informationen sieht. Das ist die gleiche Vorgehensweise wie bei einem psychiatrischen Gutachten. Denn durch das Zusammentragen der recherchierten OSINT-Daten kann unter Umständen ein komplettes Persönlichkeitsprofil entstehen.

b) Hauptverfahren

Eine rechtliche Prüfung erfahren OSINT-Ergebnisse im Ermittlungsverfahren höchstens bei Notwendigkeit eines Ermittlungsrichters, ansonsten erst in der Hauptverhandlung, wobei zu diesem Zeitpunkt die OSINT-Erkenntnisse meist schon durch werthaltigere und wertvollere Beweisergebnisse überholt worden sind, die dann anstelle dieser vor Gericht präsentiert werden. Als Ausnahme zu diesem Regelfall sind die Ergebnisse der OSINT-Maßnahmen bei Strafverfahren zu Hate Speech die finalen Beweisergebnisse. Dann muss besonders auf eine saubere Aufarbeitung und rechtssichere und belastbar dokumentierte Recherche geachtet werden.

Da die Bearbeitung eines Rechtshilfegesuches Monate dauern kann, gestaltet sich die internationale Zusammenarbeit zur Erlangung von Beweisen meist mühselig und langwierig. Durch Open Source Intelligence kann dies beschleunigt und die Einhaltung des Beschleunigungsgrundsatzes im Strafverfahren garantiert werden. Dabei kann auf die Verwendung automatisierter Datensuchen und Datenbanken zurückgegriffen werden. Bis 2001 bestand die Gefahr, durch ein solches Vorgehen internationale Rechtshilfevorschriften zu verletzen, woraufhin sich 70 Staaten auf der Cybercrime Konvention in Budapest zusammengeschlossen. Artikel 32 der Konvention regelt nun, dass öffentlich aufrufbare Daten, die im Netz verfügbar sind, auch von ausländischen Partnern und Vertragsstaaten genutzt werden können, ohne dass damit in irgendeiner Form internationale Rechtshilfevorschriften verletzt werden.[6]

c) Vollstreckungsverfahren

Am Rande können OSINT-Ergebnisse auch im Rahmen der Vollstreckung relevant werden. Bei der Beantwortung der Frage, ob sich der Angeklagte an die Weisungen aus seiner Bewährung hält, können neben dem Bewährungshelfer und der Gerichtshilfe auch OSINT-Ergebnisse Aufschluss geben.

3. Probleme und Herausforderungen

a) Manipulation

Umso relevanter die OSINT-Ergebnisse für die Beweisaufnahme sind, umso wichtiger ist die Sicherstellung der Manipulationsfreiheit der Beweisergebnisse. Ein Beweiswert kann nur hoch eingestuft werden, wenn die Authentizität und Integrität der Daten garantiert werden können. Um das zu gewährleisten, wird auf Transparenz und damit einhergehend auf die Dokumentation und objektive Nachvollziehbarkeit der Beweiskette geachtet. Maßgeblich sind vier zentrale Fragen bei der Recherche: Wie werden die Daten gesichtet? Wo werden die Daten gesichtet? Wann werden die Daten gesichtet? Und was für Daten werden gesichtet? Unklar im Umgang bleibt, zu welchem Zeitpunkt im Strafverfahren die Beweisdokumentation offengelegt werden müsste: Sofort oder erst bei Zweifeln bezüglich des Beweiswertes? Zur Sicherstellung der Authentizität muss weiterhin auch bedacht werden, dass Rechercheergebnisse jederzeit aus dem Internet entfernt werden können. Eine Absicherung der Integrität kann durch automatisierte Prozesse oder das Versehen von Hashwerten erfolgen.

b) OSINT-Ergebnisse durch Private

Nicht nur die Strafverfolgungsbehörden werden in Ermittlungen aktiv, auch Private können aus verschiedenen

[6] Council of Europe, Convention on Cybercrime, 23.XI.2001, ETS 185, online abrufbar unter: https://rm.coe.int/1680081561 (zuletzt abgerufen am 6.5.2024).

Gründen ein Interesse daran haben, die Ermittlungen zu unterstützen und der Polizei und Staatsanwaltschaften mit Informationen und Tipps zu helfen. Die Sicherstellung der Manipulationsfreiheit der Daten ist bei diesen eingeführten Ergebnissen besonders schwierig, da Privatpersonen nicht den Regeln und Vorgaben der StPO unterliegen. Der Referent zieht Parallelen zu einem Urteil des *BGH* zur DSVGO, wonach auch von Privaten erlangte Ermittlungsergebnisse, die dann an die Strafverfolgungsbehörden weitergeleitet wurden, verwertbar sind.[7] Ob eine freie Übertragung dieser Rechtsprechung möglich ist, bleibt unklar. Die Manipulation von Daten ist jedenfalls auch ohne große IT-Kenntnisse jederzeit möglich.

c) Datenleaks

Das „Leaken" von wichtigen Papieren und Dokumenten kennt man vor allem aus dem Bereich der Wirtschaftskriminalität. Wurden die Daten im Netz veröffentlicht, so fallen sie grundsätzlich unter den Begriff „Open Source" und die Polizei könnte diese sammeln und verwenden. Ein Blick auf § 202d StGB zeigt, dass der Gesetzgeber die Nutzung solcher Daten durch die Strafverfolgungsbehörden billigen könnte. Auch das *BVerfG*[8] und der *EGMR*[9] haben dazu in Fällen von angekauften Steuerdaten Stellung genommen und die Verwertbarkeit angenommen. Für die Praxis ist es von erheblicher Relevanz, dass es für Private im Hinblick auf unterschiedliche Kriminalitätsformen Möglichkeiten gibt, an Whistleblower, Hinweisgeber oder Informanten eigene Informationen abzuliefern. Darauf können sich dann journalistische Berichterstattungen stützen, die wiederum „Open Source" sind, sodass sich die Strafverfolgungsbehörden daran bedienen können. Das zeigt die teilweise komplexen Wege, wie gezielte Informationen weitergetragen werden.

4. DarkWeb Monitor

Simpel ausgedrückt, ist der DarkWeb Monitor eine Suchmaschine für das Darknet. Er kann dort so viele Seiten wie möglich erfassen, um diese dann zu standardisieren und klassifizieren. Bei diesem Vorgang werden regelmäßig Screenshots der Seiten angefertigt und versucht, die relevanten Daten zu extrahieren, um sie dann durch eine Benutzeroberfläche den Strafverfolgungsbehörden zu präsentieren. Aufgrund der regelmäßigen Anfertigung von Screenshots durch das Tool, können Veränderungen und Fehler im Aufbau der Seite nachverfolgt werden. Auch im Bereich von Bitcoins ist dieser automatisierte Vorgang – meist in Verbindung mit weiteren Techniken und Tools - typisch. Bitcoin ist nach dem allgemeinen Begriffsverständnis auch „Open Source".

5. Q&A-Session

In der sich anschließenden Q&A-Session konnte *OStA Dr. Goldbeck* noch einmal einige wichtige Aspekte hervorheben. Da es keine Vorgaben und Richtlinien gibt, ist es einzelfallabhängig, wie sorgfältig und genau die OSINT-Ergebnisse recherchiert und sichergestellt sein müssen. Wobei natürlich eine höhere Sorgfalt immer wünschenswert ist. Gerade im Hinblick auf fehlendes technisches Grundverständnis von Richter:innen sowie Schöff:innen erfordert es eine intensivere Darstellung der Daten und des Gewinnungsprozesses dieser. Weiterhin wurde auf Nachfrage die rechtliche Unterscheidung und Einordnung der Nutzung eines geleakten Passworts oder dem Auffinden eines Passworts auf einem Post-It im Rahmen einer Durchsuchung vom Referenten erläutert. Bei Letzterem müssen schon einige Ermittlungsschritte erfolgt sein, da ein Ermittlungsrichter eingeschaltet wurde, während Ersteres meist auf Glück zurückzuführen ist. Irrelevant kann sein, aus welchen Gründen Daten veröffentlicht wurden, solange diese nicht offensichtlich von Dritten ohne Erlaubnis des Betroffenen online gestellt wurden.

V. Umgang mit OSINT aus Verteidigersicht von RAin Diana Nadeborn (Tsambikakis & Partner Rechtsanwälte mbB) und RA Kai Kempgens (damals kpw.berlin, heute Eisenberg König Schork Kempgens)

Als Kontrast zu den Strafverfolgungsbehörden widmeten sich die beiden nächsten Referent:innen den Problemen und Herausforderungen für Strafverteidiger:innen im Zusammenhang mit OSINT-Ergebnissen. Die Arbeit der Strafverteidigung umfasst sowohl die Unterstützung von Geschädigten bei einer Anzeigeerstattung als auch klassischerweise die Verteidigung des Beschuldigten. Der Vortrag beschäftigt sich mit Letzterem.

Zuerst gehen die Referenten in ihrem Vortrag auf zwei unterschiedliche Quellen von OSINT-Ergebnissen im Strafverfahren (Social Media und Kundenbewertungen) ein, um dann mögliche Probleme in der Hauptverhandlung darzulegen und zuletzt noch einen Ausblick auf zukünftige Herausforderungen zu geben. Der Vortrag erfolgte durchweg mit anschaulichen Beispielen aus dem Berufsalltag der beiden.

1. Social Media

a) Richter:innen

Ein verhältnismäßig aktueller und bekannter Fall ist der sog. „Facebook-Richter" Fall.[10] Während eines Verfahrens hatte der Vorsitzende Richter ein Foto auf einer Social-Media Plattform hochgeladen, auf welchem er ein T-shirt mit den Worten „wir geben ihrer Zukunft ein zu Hause, JVA" anhatte. Darunter hatte er den Kommentar „Das ist mein, wenn du da rauskommst, bin ich in Rente, Gesicht" gepostet. Über Screenshots hatte die Verteidigung den Vorfall in den Prozess eingebracht und einen Befangenheitsantrag gestellt, welcher in der Revision vom *BGH* auch als begründet angesehen wurde. Die OSINT-Ergebnisse wurden dabei durch das Freibeweisverfahren in den Prozess eingeführt und dann durch den Richter selbst verifiziert.

---

7 *BGH*, Beschl. v. 18.8.2021 – 5 StR 217/21.
8 *BVerfG*, Beschl. v. 9.11.2010 – 2 BvR 2101/09.
9 *EGMR*, Urt. v. 6.10.2016 – 33696/11, K.S. und M.S. v. Germany.
10 *BGH*, Beschl. v. 12.1.2016 – 3 StR 482/15.

b) Angeklagte

Der Angeklagte kann in unterschiedlichen Verfahrensstadien mit OSINT-Ergebnissen in Berührung kommen. Zum Beispiel bei der Ermittlung, ob ein Grund zur Aussetzung des Verfahrens vorliegt. In einem Praxisfall gab der Angeklagte an, eine psychosomatische Lähmung zu haben, die ihn als verhandlungsunfähig einstufen würde.

Ein Sachverständiger muss sich bei der Diagnose dieser Krankheit überwiegend auf die Aussagen des Betroffenen verlassen, da das Krankheitsbild schwer nachprüfbar ist. Durch das Auffinden von Online-Fotos des Angeklagten beim Segeln konnte dessen Verhandlungsfähigkeit doch festgestellt und die Hauptverhandlung durchgeführt werden. Problematisch ist jedoch die Einführung von OSINT-Ergebnissen in die Verhandlung, wenn sie nicht authentisch und integer sind. Es besteht zwar die Möglichkeit der Bilderrückwärtssuchfunkton von Google, fraglich bleibt jedoch, was die Konsequenz wäre, wenn der Irrtum oder die Manipulation nicht aufgeklärt werden kann. Da OSINT-Ergebnisse meist nur Indizien sind, finden diese meist keine bis kaum eine Erwähnung im Urteil. Beispielsweise ist das Gericht bei der Ermittlung des Strafmaßes und der Schätzung der Tagessatzhöhe auf die Angaben des Angeklagten angewiesen. Verwenden Richter:innen das Internet im Vorfeld, um sich ein konkretes Bild zu den Lebensumständen des Angeklagten zu machen, ist das nicht nachweisbar, weil es keine Erwähnung im Urteil findet und etwaige Onlinelügen können durch den Angeklagten nicht mehr richtiggestellt werden.

c) Zeugen

Auch Zeugen können von OSINT-Ergebnissen betroffen sein. Bei der Bewertung der Glaubwürdigkeit können durch gezielte Onlinerecherchen Lügen aufgedeckt werden. In einem Fall aus dem Anwaltsalltag konnte so eine bestehende Beziehung zwischen den Nebenklägern und dem bis dato als neutral geltenden Zeugen aufgedeckt werden. Durch die Widerlegung seiner Neutralität musste der Beweiswert seiner Aussage deutlich niedriger bewertet werden.

d) Zwischenfazit

Es ist unzweifelhaft, dass die Verfahrensbeteiligten in Gerichtsverfahren ständig mit öffentlich zugänglichen Informationen konfrontiert werden. Dabei wird oft die Subjektivität der Social Media Daten übersehen und sie werden mit objektiven Informationen gleichgesetzt. Weitere Ermittlungen und Entscheidungen der Ermittlungsbehörden beruhen dann auf diesen subjektiven Vorermittlungen.

2. Handelsplattformen

Am Beispiel von Strafverfahren über Handelsplattformen wird deutlich, welche Aussagekraft öffentlich zugängliche Beiträge und Kommentare besitzen. In einem Beispiel aus dem Berufsalltag der Referentin wurde dargestellt, wie der Umfang eines Betäubungsmittelhandels über die Käuferbewertungen errechnet werden sollte. Dabei muss jedoch beachtet werden, dass auch beim illegalen Handel Käuferbewertungen von enormer Bedeutung sind, aber genauso wie beim legalen Handel nicht jede Bewertung auf einen echten Kunden zurückzuführen ist. Äußerungen und Bewertungen erfolgen in bestimmten Kontexten und durch ein Herausreißen aus diesen können sie einen anderen Aussagegehalt entfalten. Bei der Verwendung dieser ist darauf strengstens zu achten und es sollte stets eine Überprüfung des Aussagegehalts vorgenommen werden.

3. Hauptverfahren

a) Verteidigung

Es ist Aufgabe und Rolle der Verteidigung, Beweise, die in das Verfahren eingeführt werden sollen, kritisch zu hinterfragen und auf den tatsächlichen Gehalt und die Verlässlichkeit zu überprüfen und möglicherweise Korrekturen in der Aussagekraft aufzuzeigen. In wenigen Fällen geht es dabei um die Zulässigkeit vor Gericht und um Beweisverwertungsverbote. Selbst wenn Probleme bei der Beweiserhebung nachgewiesen werden können, ist die Annahme eines Beweisverwertungsverbots eine Ausnahme. Zum angemessenen Umgang mit OSINT-Beweisergebnissen können Parallelen zur IT-Forensik mit Speichermedien gezogen werden. Dort werden Ursprungsdaten gesichert, notwendige Vorkehrungen getroffen, um eine Veränderbarkeit der Daten auszuschließen, der Auswertungsweg wird dokumentiert, sodass man die Ergebnisse und deren Verwertung nachvollziehen kann. Der Erkenntnisweg muss für alle Verfahrensteilnehmer nachvollziehbar sein, damit der Weg zu anderen Interpretationsmöglichkeiten offenbleibt. Kommen andere mögliche Ergebnisse in Betracht, so senkt diese Erkenntnis den Beweiswert. Mit OSINT einhergehende Probleme sind die hohe Quellen-Diversität, die schwere Nachprüfbarkeit und die Einführung von Informationen, die mit ganz anderen Intentionen geäußert wurden. Aufgrund der Dichte und Fülle von Daten im Internet können Verteidiger den Rechercheprozess nicht selbstständig nachahmen und -empfinden. Zielführend und hilfreich wäre es, wenn nicht nur das Ergebnis, sondern auch der Gewinnungsprozess untrennbar mit dem Beweismittel verbunden ist. Dabei reicht allein die Befragung des Ermittlers zum Rechercheprozess nicht aus, sondern es braucht allgemeine Standards. Es werden derzeit verschiedene Ideen und Konzepte für Tools dafür entwickelt, jedoch noch nicht verwendet.

b) Rechtsprechung des BVerfG und des EGMR

Um das Fair-Trial Prinzip zu wahren, müssen dem Angeklagten die Recherche- und Ermittlungswege nachvollziehbar erklärt werden. Nach der Rechtsprechung des *BVerfG* ist dies Ausfluss aus dem Prinzip der Waffengleichheit.[11] Aber auch der *EGMR* hat sich dazu mit Blick

[11] *BVerfG*, Besch. v. 12.11.2020 – BvR 1616/19. Zum Zeitpunkt der Tagung noch nicht entschieden, aber die Rechtsprechung bestätigende Entscheidung *BVerfG*, Beschl. v. 23.6.2023 – 2 BvR 1167/20.

auf das Fair-Trial Prinzip und Art. 6 EMRK geäußert und stellt hohe Maßstäbe an eine Einhaltung.[12] Demnach braucht die Verteidigung nicht nur die Möglichkeit der Einsichtnahme des Rechercheprozesses, sondern auch die Gelegenheit der wirksamen Stellungnahme zu den Beweismitteln. Somit hätte die Verteidigung nicht nur die Teilhabe an den Endbeweisergebnissen, sondern auch die Chance, am Beweisermittlungsweg mitzuwirken. Der *EGMR* fordert für die Garantie der Waffengleichheit nicht nur den Zugang zu den entsprechenden Informationen, sondern vielmehr, dass Dokumentation und Stellungnahmen Standard sind. OSINT-Ergebnisse müssen für die Verteidigung so transparent sein, dass sie diese sowohl nachvollziehen als auch darauf Einfluss nehmen können.

4. Fazit

In der Praxis ist es noch mit vielen Hürden und Hindernissen verbunden, an Rohdaten zu gelangen. Geklärt ist auch nicht, was bei „Verfahrensverstößen" passieren würde, wie zum Beispiel einer fehlenden Protokollierung. Auch wenn keine Beweisverwertungsverbote vorliegen würden, würde es Auswirkungen auf den Beweiswert haben. Es besteht ein ganz erheblicher Regelungs- und Standardisierungsbedarf. Eine Regelung zur Protokollierung findet man zwar in § 100a Abs. 6 StPO, fraglich ist jedoch, ob sich diese Verpflichtung auf andere Ermittlungsmaßnahmen übertragen lässt. Wie sind die Beweisregeln? Und werden sich zuerst die Gerichte oder doch die Ermittlungsbehörden mit der Einführung von Mindeststandards befassen? Die Referenten sind sich jedenfalls sicher, dass der *BGH* und/oder das *BVerfG* in Zukunft dazu Stellung nehmen müssen.

5. Q&A-Session

Auch an diesen Vortrag schloss sich eine informative Q&A-Session an, innerhalb welcher angesprochene Aspekte aus dem Vortrag vertieft diskutiert werden konnten. Die Frage, ob nicht aufgrund der Amtsaufklärungspflicht der Gerichte und sonstigen Beweiswürdigungsvorgaben des *BGH* die Aufklärung des Beweiswertes genügend gesichert ist, wurde mit dem Hinweis auf die hohen Anforderungen an eine Aufklärungsrüge verneint. Die Nachvollziehbarkeit des Rechercheprozesses braucht es vor allen Dingen bei entscheidungserheblichen Beweisen und insoweit ist das Bewusstsein in der Praxis noch nicht angekommen. Für eine faire Verteidigung können URLs wichtig sein und OSINT-Ergebnisse müssen auch bei den Vorermittlungen bei gerichtlichen Anträgen wie Durchsuchungsanordnungen nachvollziehbar sein. Es ist sowohl Aufgabe und Rolle der Verteidigung als auch des Gerichts, die einzelnen Schritte nachvollziehen zu können, um diese im Urteil plausibel darzustellen. Die Authentizität der Beweise ist derzeit in der Praxis noch unproblematisch, da sie durch Zeugen verifiziert werden kann. Die Protokollierungspflicht aus dem europäischen Datenschutzrecht könnte sehr gut zur Gestaltung von Grundlagen in der StPO herangezogen werden. Zu begrüßen wäre auch die weitere Investition in die OSINT-Ausbildung von Beamt:innen.

[12] *EGMR*, Urt. v. 9.11.2018 – 71409/10, Beuze V. Belgium.

VI. Verändert OSINT den internationalen Kampf für Menschenrechte? Von Prof. Dr. Katrin Kinzelbach (Friedrich-Alexander-Universität Erlangen-Nürnberg)

Last but not least schloss die Referentin *Prof. Kinzelbach* die Tagung mit ihrem Vortrag ab. Dabei führte sie das Publikum weg von der juristischen Perspektive, hin zum Bereich der Menschenrechtsverletzungen. Hier ist der Bezug zu Open Source Ermittlungen bzw. Untersuchungen hochaktuell.

1. Einführung

Nicht nur bei grenzüberschreitenden Ermittlungen, wie man in den vorherigen Vorträgen hören konnte, sondern auch im Rahmen der Menschenrechtsverletzungen ist OSINT eine effektive Methode. Man kann das Vorgehen der Aktivist:innen grundsätzlich in zwei Arten unterteilen. Sog. „Bottom-up" Perspektive, bei welcher Aktivist:innen, Journalist:innen und Betroffene gemeinsam daran arbeiten, tatsächliche Informationen zu sichern oder die „Surveillance von oben" durch die Verwendung von Satellitenbildern. Dabei ist es von immenser Bedeutung, dass die Informationen verlässlich sind. Diese gelangen nämlich an verschiedene Akteure: Presse, Regierungsvertreter:innen, Gericht, UN, oder auch nationale Menschenrechtsorganisationen oder Menschenrechtsanwält:innen. Die Informationen werden demnach nicht nur juristisch verwertet, sondern vor allem auch politisch. Politische Entscheidungsträger und die Weltöffentlichkeit spielen die tragende Rolle im Kampf gegen Menschenrechtsverletzungen.

Der Vorgang zum Publikmachen von Menschenrechtsverletzungen gestaltet sich wie folgt: Im Land werden aufgrund repressiver Politik verschiedene Organisationen oder Institutionen unterdrückt. Diese versuchen sich dagegen aufzulehnen und suchen Verbündete im Ausland zur Zusammenarbeit. Diese Verbündeten haben im Idealfall Kontakte zu anderen, möglichst mächtigen Staaten oder auch zu internationalen Organisationen.

2. Historie und Entwicklung

Durch die Entwicklung des Internets und den sich daraus ergebenden neuen Möglichkeiten hat sich der Kommunikationsweg der Menschenrechtler im Laufe der Zeit gewandelt. Ein Umbruch begann 1966 durch die Verabschiedung des großen Menschenrechtspakts, welcher zehn Jahre später in Kraft trat. Die Menschenrechtspakte stellen ein Versprechen der Staaten dar, dass die eigenen Bürger:innen nach bestimmten Standards behandelt werden sollen. Da es kein Gericht auf internationaler Ebene gab, war die einzige Hoffnung von Betroffenen, dass die Vorfälle und Szenen in der Welt veröffentlicht werden, um die politische Maschinerie in Gang zu setzen. Ein wichtiger Meilenstein und eine große Veränderung der Kommunikation war die Erfindung und dann auch der Verkauf des Faxes an private Organisationen. Eine Verbreitung und

Veröffentlichung der Verbrechen konnte durch die damaligen Technologien zwar zeitnah, jedoch nur zeitversetzt erfolgen. Dies änderte sich im Jahr 1993. In diesem Jahr wurde der Pakt der Menschenrechte in Wien bestätigt und im selben Jahr das WorldWideWeb an die Öffentlichkeit freigegeben. Die neuen Technologien haben die Vernetzung vorangetrieben, da Einzelpersonen nun selbst mit der Welt Daten und Informationen teilen können und mittlerweile Menschenrechtsverletzungen live veröffentlicht werden können.

3. OSINT als zweischneidiges Schwert

Auf der einen Seite können durch Open Source Intelligence extrem viele Informationen erfasst werden, auf der anderen Seite bestehen weitläufige Überwachungsmöglichkeiten. Es werden Informationen blockiert, beseitigt, bestritten und die Richtigkeit und Authentizität bezweifelt. Zusätzlich werden durch Menschenrechtsgegner Desinformationen gestreut, was zu Verunsicherung und Verwirrung führt. Daneben arbeiten diese mit massiver Einschüchterung durch Androhung mit politischer Haft, „Verschwindenlassen" bis hin zum Mord. Die Arbeit der Menschenrechtsorganisationen umfasst in der Regel Interviews mit den Betroffenen, wobei diese Aussagen dann verifiziert werden müssen. Welche Schwierigkeit bei der Überprüfung der Aussageinhalte besteht, hat sich im Jahr 2017 am Beispiel *Bashar al-Assad* gezeigt.[13] Diesem wurde umfassende Folter in einem Militärgefängnis vorgeworfen. Im Rahmen seiner Befragung verneinte er die Situation und stellte die Integrität und Authentizität der digitalen Beweise in Frage. Da eine Beweissicherung vor Ort durch unabhängige Beobachter nicht möglich war, konnte der Menschenrechtsgegner diese Schwäche gezielt ausnutzen.

4. Die Rolle von Privaten und einhergehende Hindernisse

Menschenrechtsorganisationen haben die Möglichkeit, weitere Bild- und Videodateien durch freiwillige Helfer und Einzelpersonen zu erlangen. Wie aber aus den vorherigen Vorträgen hervorging, kann die Verwendung und Verwertung der Materialien von Privatpersonen problematisch sein. Die Motivation dieser kann aus unterschiedlichen Beweggründen entstehen. Neben der eigenen Betroffenheit kann es auch um die Aufarbeitung der Geschehnisse gehen und das Festhalten für die nächsten Generationen.

a) Organisation zur Unterstützung

Es gibt einige Organisationen, die sich mit der Unterstützung von Menschenrechtsaktivist:innen durch Private befassen. Eine davon ist „Witness". Diese bilden Private zur richtigen Erstellung von OSINT-Material aus, sodass es zum einen für die Menschenrechtsorganisationen verwendbar ist, aber sich zum anderen die freiwilligen Helfenden nicht in Gefahr bringen. In Hongkong beispielsweise hat die Polizei starke Taschenlampen eingesetzt, um das Bildmaterial unbrauchbar zu machen. In anderen Staaten ist die Lage jedoch deutlich angespannter und es kommt zu Gewalt. Witness will Lösungen für diese Szenarien finden. Eine andere Organisation ist Syrian Archives. Sie sichten und speichern Videos, die über Syrien und den Zustand vor Ort auf Youtube hochgeladen wurden, da der Algorithmus diese aufgrund der Gewaltdarstellung löschen würde. Durch dieses Vorgehen können jedoch auch Metadaten der Materialien, die Aufnahmezeit und -ort enthalten, verloren gehen. Zur Überprüfung und Verifikation müssen dann weitere Quellen herangezogen werden, was bei einem manuellen Vorgehen mühselig sein kann. Aufgrund der bestehenden Ressourcenprobleme ist eine Automatisierung in diesem Bereich notwendig. Manuell sind solche Massendaten kaum zu bewältigen. Mittlerweile gibt es Apps, die entwickelt wurden, um das Teilen von Fotos und Videos zu erleichtern, ohne dass Metadaten verloren gehen. Zudem gab es in Yale ein Projekt mit Studierenden, die Tools zur Automatisierung der Sichtung getestet und einen Bericht dazu verfasst haben. Die Entwicklung gestaltet sich dementsprechend positiv und fortschrittlich, um die Rechercheprozesse in Zukunft zu verbessern und zu erleichtern.

b) Ressourcenprobleme

Zu OSINT gehören auch öffentlich zugängliche Satellitenbilder und Geodaten. Zur Bewältigung dieser Massendaten wollte Amnesty International freiwillige Helfer einbinden, um das Material zu sichten und zu codieren. Durch eine unabhängige Sichtung der Einzelpersonen wollte man eine verlässliche Überprüfung garantieren. Problematisch war jedoch die damit einhergehende psychische Belastung, die von der Organisation nicht vorhergesehen wurde. Die Helfenden konnten nicht angemessen darauf vorbereitet werden, um sich entsprechend abzugrenzen. Sie wurden dann durch die Satellitenbilder, die angezündete und geplünderte Dörfer zeigten, teilweise traumatisiert. Das wiederum führt dazu, dass die Sichtung nicht mehr auf freiwillige Helfende übertragen werden konnte, sondern intern durchgeführt werden musste.

c) Das Berkeley Protokoll

Ein weiterer Lösungsansatz zur Unterstützung von freiwilligen Helfenden und der Standardisierung des Vorgehens bei OSINT-Investigations stellt das Berkeley Protokoll dar. Das Protokoll will wichtige Fragen beantworten: Wie kann OSINT tatsächlich sinnvoll in der Menschenrechtsarbeit eingesetzt werden? Wie gehen wir mit Privatsphäre um und wie müssen die Daten gesichert werden? Wie kann Authentizität überprüft werden? Das Berkeley Protokoll soll als Anleitung dienen, wie man insbesondere mit Foto- und Videomaterial, aber auch mit anderen Open Source Recherchen im Internet vernünftig umgehen kann. Es richtete sich dabei sowohl an Ermittelnde

[13] ECCHR, Dossier, Menschenrechtsverbrechen in Syrien: Folter unter Assad, März 2021, online abrufbar unter: https://www.ecchr.eu/fileadmin/Sondernewsletter_Dossiers/Dossier_Syrien_2021Maerz.pdf (zuletzt abgerufen am 6.5.2024).

als auch an Einzelpersonen oder Menschenrechtsorganisationen. Dabei handelt es sich um Pionierarbeit, die gerade im Hinblick auf die technischen Aspekte noch am Anfang steht.

5. Beispiel

Ein sehr spannendes und interessantes Beispiel zur Nutzung von OSINT durch Private und die Bedeutung der Informationen, die dadurch gewonnen werden, zeigt sich am Beispiel Xingjiang, einer nordöstlichen Region in China. Hier wurden durch die Zusammenarbeit eines Individuums, den Menschenrechtsorganisationen und Journalist:innen Menschenrechtsverletzungen aufgedeckt. Zum Zeitpunkt, als Gerüchte über Masseninternierung in China laut wurden, wurde der chinesische Staatsbürger *Shawn Zhang*, der mittlerweile in Kanada lebte und studierte, darauf aufmerksam. Er wollte die Gerüchte eigentlich widerlegen. Nachdem er jedoch im Internet Bauanträge für Lager fand, nutze er Google Earth, um die Lokalisationsdaten, die er aus den Anträgen entnehmen konnte, zu überprüfen. Tatsächlich fand er die Lager. Der Staat hat eine solch dezentralisierte Recherche nicht vorausgesehen und zu diesem Zeitpunkt keine Verschleierung vorgenommen. Danach wurden die Plätze als Sporthallen und Schulen getarnt. Auch Journalist:innen wurden aufmerksam und recherchierten. Benutze man die chinesische Suchmaschine, so sah man teilweise verschwommene und verpixelte Stellen. Suchte man die gleichen Stellen jedoch über andere Suchmaschinen, so konnte man die errichteten Lager sehen. Somit hatte die Zensur das Gegenteil bewirkt und beim Auffinden geholfen. Unabhängig davon hatten Menschenrechtsorganisationen Interviews mit Betroffenen durchgeführt. Die Satellitenbilder von *Shawn Zhang* hatten in diesem Zusammenhang eine enorme Bedeutung, denn sie konnten die Interviews letztlich verifizieren in einer Gegend, in welcher das Auffinden oder Erstellen von nutzergenerierten Daten schwer ist. Die Kombination der Quellen und das gegenseitige Bestätigen der Aussagen führte zu einem kritischen Blick auf China und motivierte weitere Akteure, Beweise zur Bekräftigung zu finden. Dies zeigt, dass es trotz neuer technologischer Möglichkeiten immer noch Gegenden gibt, die schwer erreichbar sind und in denen systematisch Menschenrechtsverletzungen stattfinden können.

6. Ausblick

Ein wichtiger Moment der letzten Jahre war der Haftbefehl gegen *Al-Werfalli* in Lybien, welcher fast ausschließlich auf Open Source Material beruhte.[14] Das hat auch bei kleineren Organisationen für Hoffnung gesorgt, denn zuvor konnten Kriminelle das Internet zur Selbstdarstellung und zur Verbreitung von Terror und Angst nutzen, da durch die geringe Ahndung im Netz der Eindruck eines rechtsfreien Raums vermittelt wurde. Auf der anderen Seite basieren die Recherchen der Menschenrechtsaktivist:innen darauf, dass die Täter:innen freiwillig mit ihren Taten angeben und diese im Internet hochladen. Dieses Vorgehen könnte sich zukünftig ändern, wenn sich den Täter:innen offenbart, dass sie sich damit selbst schaden.

7. Q&A-Session

In der letzten Q&A-Session des Tages wurde darüber gesprochen, wie man die Ressourcen von Menschenrechtsorganisationen erweitern kann, z.B. durch Kooperationen oder einem Secure Drop im Darknet. Dabei erläuterte die Referentin, dass es durchaus eine technikaffine und versierte Szene unter den Menschenrechtsaktivist:innen gibt, die nicht nur das sichere Uploaden von Dateien überblickt, sondern auch, welche Informationen konkret hochgeladen werden können und sollen. Zu bewältigen bleibt jedoch weiterhin das Problem, wie eine Mithilfe durch Laien und freiwillige Helfende gewährleistet werden kann, ohne dass sich diese in akute Gefahr begeben.

VII. Schlussworte und Fazit

Auch wenn der Begriff OSINT den meisten im Alltag eher unbekannt ist, so handelt es sich dabei um eine Technik, die jeder intuitiv anwendet, um Informationen zu erlangen. Die rechtlichen und tatsächlichen Hindernisse, die sich in der Dogmatik, Justizarbeit, bei der Strafverteidigung und der internationalen Arbeit von Menschenrechtsorganisationen zeigen, wurden durch viele spannende Beispiele in den Vorträgen anschaulich erklärt, sodass die Teilnehmer:innen den Wassersaal der Orangerie abends mit einem besseren Bewusstsein für Open Source Intelligence verlassen konnten. Die jeweiligen sich an die Vorträge anschließenden Q&A-Sessions wurden sowohl vor Ort als auch online dankbar genutzt. Zudem konnten sich die Anwesenden, Mitwirkenden und Expert:innen mit Fragen, Impulsen und Anregungen auch während des Stehempfangs oder der Mittags- und den Kaffeepausen in einer lockeren Atmosphäre vertieft auseinandersetzen. Die Bedeutung der interdisziplinären Vernetzung und die Verzahnung von Praxis und Wissenschaft spiegelte sich auch in den Vorträgen wider, da die Referent:innen häufig wechselseitig aufeinander Bezug nahmen. *Prof. Dr. Christoph Safferling*, LL.M. (LSE) und sein ICLU-Team freuen sich über die rege Teilnahme und lebhafte Interaktion der Teilnehmenden und die Fortsetzung der Veranstaltungsreihe auch im Jahr 2024, dann zum Thema Hate Speech im Internet.

[14] Prosecutor vs. Al-Werfalli (Warrant of Arrest) ICC-01/11-01/17 (15 August 2017, online abrufbar unter: https://www.icc-cpi.int/sites/default/files/CourtRecords/CR2017_05031.PDF (zuletzt abgerufen am 6.5.2024).