RISIKO

GRUNDLAGEN

Kinder und Jugendliche im Umfeld von Gewalt – Aufgaben und Möglichkeit der Jugendstrafrechts-pflege
[Alexandra Ott Müller / Sven Zimmerlin]

POLIZEI & MILITÄR

Staatshaftung im Rahmen der Erfüllung sicherheitspolizeilicher Aufgaben durch Private
[Andrea Selle]

TECHNIK & INFRA-STRUKTUR

Rechtmässigkeit von Open Source-Ermittlungen durch Strafverfolgungs-behörden
[Monika Simmler / Giulia Canova]

RISIKO & RECHT AUSGABE 01 / 2024

RECHT

Rechtmässigkeit von Open Source-Ermittlungen durch Strafverfolgungsbehörden

Monika Simmler / Giulia Canova*

Die Nutzung öffentlich zugänglicher Informationen („Open Source Information") durch Strafverfolgungsbehörden mag auf den ersten Blick unproblematisch erscheinen, ist jedoch strafprozessrechtlich nicht unbedenklich. Die Bearbeitung von Personendaten im Rahmen von „Open Source Intelligence" (OSINT) berührt Art. 13 Abs. 2 BV. Das Vorliegen einer Einwilligung durch die Veröffentlichung der Informationen schliesst die Qualifikation als Grundrechtseingriff nicht aus und lässt das Erfordernis einer gesetzlichen Grundlage nicht entfallen, reduziert die Invasivität der Massnahme aber deutlich. Wie diese Abhandlung darlegt, lässt sich allerdings nicht bei jeder OSINT-Methode auf eine Einwilligung schliessen. Einfaches und generatives Web Crawling sind von Web Scraping oder intelligenten Datenweiterberarbeitungen zu unterscheiden. Bei der Beurteilung der Invasivität von OSINT-Massnahmen sind ferner ihr Zweck, die Art der bearbeiteten Daten und zu überwindende technische Hürden einzubeziehen. Die Auseinandersetzung mit den strafprozess-, verfassungs- und konventionsrechtlichen Grundlagen zeigt, dass das geltende Recht nur minimalinvasive Open Source-Recherchen, nicht jedoch eingriffsintensivere Massnahmen abdeckt. Eine explizite innerstaatliche Regulierung wäre in Anbetracht der Praxisrelevanz dieser Ermittlungsmethode angezeigt.

* Prof. Dr. Monika Simmler ist seit April 2021 Assistenzprofessorin für Strafrecht, Strafprozessrecht und Kriminologie sowie Co-Direktorin des Kompetenzzentrums für Strafrecht und Kriminologie an der Universität St. Gallen. Sie hat 2017 an der Universität Zürich promoviert und war von 2016 bis 2018 als Gastforscherin an der Columbia University, der University of Oxford und an der Universität Wien tätig.
Giulia Canova hat Law and Economics an der Universität St. Gallen studiert. Seit 2022 ist sie wissenschaftliche Mitarbeiterin und Doktorandin am Kompetenzzentrum für Strafrecht und Kriminologie an der Universität St. Gallen. Sie forscht zur strafprozessrechtlichen Regulierung digitaler Ermittlungen.

Inhalt

I. Einleitung

Im Jahr 2024 stieg die Zahl aktiver Internet-Nutzerinnen weltweit auf über fünf Milliarden.[1] Sie generieren mit ihrem Online-Verhalten immer mehr Daten, die im Netz brachliegen. Ein Grossteil dieser Daten ist ohne besondere Vorkehren zugänglich, womit das Internet für Strafverfolgungsbehörden zu einer potenten Informationsquelle wird.[2] Open Source Information (OSINF), d.h. öffentlich zugängliche Informationen, werden in Ermittlungen regelmässig zur Aufklärung von Straftaten genutzt.[3] OSINF lässt sich über einfache Suchabfragen oder mittels spezifischer Software der Open Source Intelligence (OSINT) nutzbar machen. Mit OSINT werden Informationen automatisiert gesammelt und verarbeitet, insbesondere gestützt auf Web Crawling- und/oder Web Scraping-Methoden. Die Bandbreite existierender Anwendungen ist allerdings gross: Sie reicht von Google- oder ChatGPT-Abfragen über automatisierte Analysen von Social Media-Netzwerken hin zur Bildersuche gestützt auf Gesichtserkennungstechnologie.

Ermittlungen gründen auf Informationsbeschaffung. OSINT ist ein ressourcenschonender Weg, relativ einfach an viele Informationen zu gelangen. Da es sich bei OSINF um (sensible) Personendaten handeln kann, ist deren Bearbeitung mit Blick auf den Grundrechtsschutz nicht per se unproblematisch. Die Beschaffung von Personendaten wie Fotos, E-Mails oder Social Media-Posts sowie die mit der Abfrage einhergehende Datenbekanntgabe berühren den Schutzbereich von Art. 13 Abs. 2 BV[4], dem sog. „Recht auf informationelle Selbstbestimmung". Es ist fraglich, ob die öffentliche Zugänglichkeit der Informationen als Einwilligung in die behördliche Datenbearbeitung zu interpretieren ist, wie sich dies auf die Qualifikation der Massnahme als Grundrechtseingriff auswirkte und ob dennoch eine gesetzliche Grundlage erforderlich wäre.

Die strafprozessrechtliche Einordnung von OSINT ist bis anhin kaum diskutiert. Für die Schweiz existiert – bis dato – nur eine Abhandlung zur Einordnung von Google-Suchen.[5] In Deutschland ist die Diskussion bereits etwas

---

1 Statista, Number of internet and social media users worldwide as of January 2024, abrufbar unter <https://www.statista.com/statistics/617136/digital-population-world-wide/#:~:text=As%20of%20July%202023%2C%20there,population%2C%20were%20social%20media%20users>.

2 Cartner/Schweingruber, 990.

3 Rückert, Online-Streife 302; Cartner/Schweingruber, 990.

4 Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (BV, SR 101).

5 Cartner/Schweingruber, 990 ff.

ausgereifter.[6] Während die Schweizer Publikation von CARTNER und SCHWEINGRUBER davon ausgeht, dass Strafverfolgungsbehörden ohne weiteres Googeln dürfen,[7] nimmt RÜCKERT für das deutsche Recht an, dass mit gewissen OSINT-Methoden teilweise gar schwere Grundrechtseingriffe einhergehen, die neue gesetzliche Grundlagen erforderlich machen.[8]

Die vorliegende Abhandlung will zunächst klären, ob und inwiefern die strafprozessuale Beschaffung öffentlich zugänglicher Informationen einen Grundrechtseingriff darstellt. Dafür sind die Grundlagen von OSINF und OSINT zu erläutern (Kap. II) und verschiedene Kategorien zu unterscheiden (Kap. III). Anschliessend sind diese Methoden grundrechtlich zu qualifizieren und die Wirkung sowie Reichweite mutmasslicher Einwilligungen zu diskutieren (Kap. IV). Da sich zeigt, dass auf das Erfordernis einer gesetzlichen Grundlage nicht verzichtet werden kann, sind mögliche Rechtsgrundlagen zu analysieren (Kap. V). Infrage kommen eine allgemeine „Ermittlungsgeneralklausel", die internationale Convention on Cybercrime (CCC) oder spezifische Zwangsmassnahmen wie die Observation. Ein Fazit rundet den Beitrag ab (Kap. VI).

II. Open Source Intelligence

1. Begriffe

Open Source Information bedeutet schlicht „öffentlich zugängliche Information". Der Terminus der Open Source Intelligence hingegen entstammt der Kriminalistik und bezeichnet die (zunächst von Geheimdiensten genutzte) Methode, mit der entsprechende Daten für Ermittlungen gewonnen werden können.[9] Was jedoch unter öffentlich zugänglichen Daten zu verstehen ist, ist weder im Strafprozess- noch im Datenschutzrecht legaldefiniert.[10] Auch aus der

---

6 Siehe die Beiträge von RÜCKERT, Online-Streife, 302 ff.; RÜCKERT, Verbrecherjagd; WITTMER/PLATZER, 569 ff.; BIERESBORN, 319.

7 CARTNER/SCHWEINGRUBER, 990 ff.

8 RÜCKERT, Online-Streife, 302 ff.

9 LUDEWIG/EPPLE, 457 ff.; WITTMER/PLATZER, 751.

10 Art. 13 des Bundesgesetzes über den Nachrichtendienst vom 25. September 2015 (Nachrichtendienstgesetz, NDG, SR 121) hält immerhin fest, dass „öffentliche Informationsquellen" namentlich öffentlich zugängliche Medien, öffentlich zugängliche Register, von Privaten öffentlich zugänglich gemachte Personendaten und in der Öffentlichkeit vorgetragene Äusserungen umfassen.

Literatur ergibt sich nicht eindeutig, wo die Grenze zwischen öffentlich zugänglichen und nicht-öffentlichen Informationen liegt.[11]

CARTNER und SCHWEINGRUBER schlagen zur Konturierung des Begriffs vor, Daten als öffentlich zugänglich anzusehen, wenn diese aus frei verfügbaren, offenen Quellen stammen. Dazu würden den Autorinnen zufolge alle im Internet zugänglichen Informationen gehören, die von der Suchmaschine Google indexiert werden und über einfache Recherchen erhältlich sind. Demgegenüber seien Daten nicht mehr öffentlich, wenn sie einem begrenzten Kreis von Nutzerinnen vorbehalten sind, bspw. wenn es einer „Follower-" oder „Freundschaftsanfrage" bedarf.[12]

Nach der Rechtsprechung des deutschen Bundesverfassungsgerichts umfassen öffentlich zugängliche Informationen sämtliche Kommunikationsinhalte, die sich an jede Person oder zumindest an einen nicht weiter abgegrenzten Personenkreis richten.[13] Basierend auf dieser Rechtsprechung sind gemäss RÜCKERT Daten öffentlich zugänglich, wenn sie im Internet für jede Person abrufbar sind.[14] Offensichtlich davon erfasst seien alle Informationen im offenen Teil des Internets (sog. Surface Web), die von Standardsuchmaschinen indexiert und somit von jeder Internetnutzerin ohne Weiteres auffindbar sind. Ebenfalls öffentlich zugänglich seien Daten im sog. Deep Web („unter" der Schicht des offenen, indexierten Bereich des Internets), die von Suchmaschinen nicht indexiert sind, aber aufgefunden werden können, wenn die genaue Web-Adresse bekannt ist.[15] Aber auch Daten im Dark Web, welche nur über bestimmte Anonymisierungssoftware (wie den Tor-Browser[16]) zugänglich sind, gelten RÜCKERT zufolge als öffentlich, da sie für jede Internetnutzerin zugänglich bleiben.[17] Jenseits dieser Sphäre würden hingegen individuelle Kommunikationsinhalte liegen, die bewusst nur an bestimmte Personen gerichtet sind.[18]

---

11 CARTNER/SCHWEINGRUBER, 991; vgl. HARASGAMA, 246; vgl. RÜCKERT, Online-Streife, 310 ff.; WITTMER/PLATZER, 571 ff.

12 Zum Ganzen CARTNER/SCHWEINGRUBER, 991.

13 BVerfGE, Urteil vom 27. Februar 2008, 120, 274 („Online-Durchsuchung"), Rz. 308 f.

14 RÜCKERT, Online-Streife, 310.

15 RÜCKERT, Online-Streife, 310; RÜCKERT, Digitale Daten, 269 f.

16 Tor ist ein Netzwerk zur Anonymisierung von Verbindungsdaten, bei dem der Datenverkehr über das Netzwerk geleitet und mehrfach verschlüsselt wird; dazu KRAUSE, 647.

17 RÜCKERT, Online-Streife, 311 f.

18 RÜCKERT, Online-Streife, 312; BVerfGe 120, 274, Rz. 308.

Wie diese Abgrenzungsversuche zeigen, geht es bei OSINT um die Verarbeitung von Informationen, die online verfügbar sind und über Suchmaschinen oder andere Tools gewonnen werden können. Die Zugänglichkeit bestimmt sich nicht allein über die verwendete Methode, womit grundsätzlich auch schwerer zugängliche Daten erfasst bleiben. Allerdings ist die Grenze einerseits dort auszumachen, wo technische oder faktische Grenzen den Zugang objektiv verunmöglichen (z.B. wenn ein bestimmtes Passwort benötigt wird oder zuerst einer Kontaktanfrage zugestimmt werden muss). Andererseits kann die Grenze subjektiv in der Erwartungshaltung der betroffenen Person begründet liegen, wenn diese berechtigterweise auf die Nichtöffentlichkeit der Information zählt.

2. Datenbeschaffung und Datenbekanntgabe

Ungeachtet des genauen Begriffsverständnisses handelt es sich bei OSINT jedenfalls um Vorgänge zur Beschaffung von Daten. Im Strafverfahren folgt die Informationsbeschaffung konkreten Verdachtslagen. Auch wenn die erlangten Informationen aus Sachdaten bestehen können (z.B. bei der Nutzung von Google Maps zur digitalen Inspektion eines Tatorts), weisen die Recherchen meist einen Bezug zu Zielpersonen (wie beschuldigten Personen oder Geschädigten) auf. Mit einer personenbezogenen OSINF-Abfrage (z.B. eine Google-Suche nach „Petra Musterfrau Lebenslauf“) werden Informationen angepeilt, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen (vgl. Art. 5 lit. a DSG[19]). OSINT involviert deshalb i.d.R. die staatliche Bearbeitung von Personendaten.[20] Als solche fällt die Massnahme in den Schutzbereich des Art. 13 BV.[21] Das in Art. 13 Abs. 2 BV verankerte Recht auf Schutz vor Datenmissbrauch gewährt einer Person, grundsätzlich selbst darüber zu bestimmen, wem und wann persönliche Informationen offenbart werden.[22]

Open Source-Ermittlungen gehen nicht nur mit einer Informationsgewinnung einher, sondern stellen im Regelfall ebenso eine Datenbekanntgabe dar. Bereits eine Google-Suche impliziert eine Datenbekanntgabe ins Ausland.[23] Suchmaschinen speichern Daten über getätigte Suchanfragen. Bei einer

---

19 Bundesgesetz über den Datenschutz vom 25. September 2020 (Datenschutzgesetz, DSG, SR 235.1).

20 Cartner/Schweingruber, 991 und 993; Rückert, Online-Streife, 313 f.

21 BGE 122 I 360, E. 5a S. 362; BSK BV-Epiney, Art. 13 Rz. 33; Kiener/Kälin/Wyttenbach, § 14 N 57.

22 Anstatt vieler Müller/Schefer, 167; SGK BV-Schweizer/Striegel, Art. 13 Rz. 79.

23 Bieresborn, 319.

Google-Suche bekommt jede Nutzerin standardmässig eine Identifikationsnummer zugewiesen.[24] Die Google-Server protokollieren diese ID bei Suchanfragen ebenso wie die IP-Adresse, den Inhalt der eingegebenen Suchanfrage sowie Datum und Uhrzeit der Anfrage, was zur Personalisierung der Suchergebnisse genutzt wird.[25] Die Datenerhebung impliziert also eine Bekanntgabe dieser Inhalte an Google.[26] Zudem prägen Suchabfragen zukünftige Suchergebnisse. Suchen Behörden im Kanton St. Gallen oft nach einer spezifischen Kombination von Begriffen (z.B. „Peter Mustermann Oster-Krawalle"), erfährt Google nicht nur, dass die Behörden diese Verknüpfung vornehmen, sondern steigt für zukünftige Suchanfragen auch die Wahrscheinlichkeit, dass Google anderen Nutzerinnen diese Kombination vorschlägt. Ähnlich verhält es sich bei einer Recherche mit Tools wie ChatGPT von OpenAI. ChatGPT ist eine Anwendung der sog. generativen Künstlichen Intelligenz (KI). Der Chatbot speichert und verarbeitet die eingegebenen Daten, um das System weiterzuentwickeln und präzisere Ergebnisse zu liefern.[27] Eine Eingabe von Informationen ist daher mit einer Datenbekanntgabe an OpenAI verbunden. Dieser Mechanismus geht mit den meisten OSINT-Anwendungen einher. Da diese Dienste zumeist von ausländischen Unternehmen angeboten werden, erfolgt die Bekanntgabe zudem i.d.R. ins Ausland, was mit spezifischen Persönlichkeitsrisiken einhergeht.[28]

Aufgrund des zweiseitigen Mechanismus aus Beschaffung und Bekanntgabe von Personendaten berühren Open Source-Ermittlungen auf zweierlei Weise den Schutzbereich von Art. 13 Abs. 2 BV. In Anbetracht der öffentlichen Zugänglichkeit der Daten steht allerdings die Frage im Raum, ob nicht in diese Bearbeitung eingewilligt wurde und deshalb kein grundrechtlicher Schutz besteht. Das etwaige Vorliegen einer Einwilligung hängt jedoch massgeblich vom Kontext der Veröffentlichung ab.[29] Nicht bei allen OSINF kann ohne Weiteres vom Vorliegen einer Einwilligung ausgegangen werden. Während dies bei einzelnen, zur Information der Allgemeinheit hochgeladenen Daten (z.B. Angaben in einer „Über mich-Spalte" einer persönlichen Webseite) der Fall sein mag, ist dies bei der Beschaffung sämtlicher im Netz auffindbarer Gesichtsbilder einer Person (z.B. über „Face Search Engines" wie PimEyes[30]) kaum mehr anzuneh-

24 Voigt, 378.
25 Becker/Becker, 351.
26 Vgl. Bieresborn, 321.
27 Mohn, 541; Woerlein.
28 Dazu OFK DSG-Glass, Art. 5 lit. e Rz. 1.
29 Vgl. OFK DSG-Steiner/Laux, Art. 30 Rz. 38.
30 Dazu Köver.

men. Problematisch erweist sich dabei auch, dass sich bei einem Grossteil der Informationen gar nicht beurteilen lässt, ob diese von der betroffenen Person selbst veröffentlicht wurden.[31] Ferner ist zu klären, ob eine Einwilligung solche Eingriffe für sich alleine überhaupt zu rechtfertigen vermag oder als Gesetzessurrogat taugt. Die Bandbreite von OSINT-Methoden lässt die pauschale rechtliche Beurteilung dieser Fragen nicht zu, weshalb es notwendig ist, konkrete Anwendungen zu differenzieren.

III. Kategorien

1. Methoden

Für die rechtliche Beurteilung ist massgeblich, wie Behörden an OSINF gelangen (Beschaffung) und welche Daten sie dabei preisgeben (Bekanntgabe). Informationen im Internet sind verteilt auf Webseiten, die mittels Web Crawling aufgefunden, indexiert und durchsucht werden können. Der Durchsuchung vorausgehen kann aber auch Web Scraping, mit dem Daten extrahiert und in Datenbanken zusammengefügt werden. Als Steigerungsform können sich Crawling und Scraping „intelligenten" Methoden bedienen, welche die Daten auf besondere Weise weiterbearbeiten.

a) Web Crawling

In erster Linie lässt sich OSINF über Suchmaschinen wie Google, Yahoo oder Bing abrufen. Solche Suchmaschinen basieren auf Datenbanken mit Listen und Zusammenfassungen von Webseiten, die durchsucht werden können.[32] Zu ihrer Erstellung werden Web Crawler eingesetzt, welche das Internet durchforsten und Webseiten indexieren.[33] Die Crawler öffnen dabei automatisiert nach vorgegebenen Kriterien bestimmte Webseiten, durchsuchen die Inhalte und öffnen vorhandene Links auf andere Webseiten, um dann den Inhalt dieser Webseite ebenso zu durchsuchen (*Crawling*).[34] Der Inhalt jeder aufgefundenen Webseite wird analysiert, um die massgeblichen Inhalte in der Datenbank zu speichern, d.h. zu indexieren (*Indexing*). In der Index-Datenbank können die zuvor gecrawlten Webseiten nach bestimmten Suchbegriffen durchsucht wer-

31 Bauer, 115 ff.; Rückert, Digitale Daten, 270.

32 Schwartz, 974.

33 Kausar/Dhaka/Kumar Singh, 31 f.

34 Web Crawler werden deshalb auch Web Robot oder Web Spider genannt, zur Funktionsweise Heydon/Najork 220; Kausar/Dhaka/Kumar Singh, 32.

den.[35] Wie die Ergebnisse zusammengestellt werden, bestimmen Algorithmen der Suchmaschine. Der Algorithmus „PageRank" von Google berechnet z.B. in einem komplexen Verfahren die relevantesten Ergebnisse.[36] Die Suchergebnisse werden zudem anhand bisheriger Aktivitäten und Informationen über die Nutzerin personalisiert.[37] Die Zuhilfenahme von Standard-Suchmaschinen ist die verbreitetste Methode, an OSINF zu gelangen.[38] Sie kann als *einfaches Web Crawling* bezeichnet werden.

Neben Standardsuchmaschinen, die nach bestehenden Webseiten crawlen, lassen sich für OSINT auch Crawling-Systeme einsetzen, die von Webseiteninhalten „lernen" und neue Inhalte generieren. Dazu gehört das generative KI-System ChatGPT, das u.a. aus gecrawlten Inhalten des Internets neue Textbestandteile erstellt. Das Large Language Modell (LLM) wurde mit einer riesigen Menge an Textdaten trainiert, um möglichst „menschliche" Texte zu generieren.[39] Die zum Training des Chatbots verwendeten Textdaten stammen (1.) aus OSINF, (2.) von Drittparteien, welche die Informationen zur Verfügung stellen oder (3.) von Nutzerinnen oder Trainingspersonen.[40] Erstere entstammen grösstenteils dem Datenset „Common Crawl", das derzeit grösste verfügbare Datenset öffentlich zugänglicher Informationen, welches als Trainingsdatenbasis für LLM dient.[41] ChatGPT wurde mit OSINF trainiert, gibt also gewissermassen auch OSINF wieder. Der Chatbot beantwortet von Nutzerinnen eingegebene Fragen oder Anweisungen („Prompts").[42] Das System generiert daraufhin passende Wortfolgen. Die Generierung basiert auf den Trainingsdaten, wobei das System aus den Konversationen stetig dazulernt.[43] Seit September 2023 verfügt es zudem über eine Online-Browse-Funktion, mit der aktuelle Informationen aus dem Internet wiedergegeben werden.[44] Chatbots wie ChatGPT sind eine Alternative zu gängigen Suchmaschinen. Da dabei die her-

---

35 Grundsätzlich zu Web Search Engines Seymour/Frantsvog/Kumar, 55.

36 Seymour/Frantsvog/Kumar, 52.

37 Bieresborn, 321.

38 Cartner/Schweingruber, 991; vgl. Rückert, Online-Streife, 310.

39 Luccioni/Viviano, 182.

40 So die Angaben von OpenAI, abrufbar unter <https://help.openai.com/en/articles/7842364-how-chatgpt-and-our-language-models-are-developed>.

41 Luccioni/Viviano, 182.

42 Woerlein, 01205.

43 So die Angaben von OpenAI, abrufbar unter <https://help.openai.com/en/articles/5722486-how-your-data-is-used-to-improve-model-performance>.

44 Medienmitteilung von OpenAI vom 27. September 2023, abrufbar unter <https://x.com/OpenAI/status/1707077710047216095?s=20>.

kömmliche Abfrage von OSINF mit Methoden der generativen KI kombiniert wird, kann bei der Methode von *generativem Web Crawling* gesprochen werden.

b) Web Scraping

Ermittlungen können sich auch Web Scraping zu Nutze machen. Beim Scraping werden bestehende Inhalte im Internet nicht bloss indexiert und durchsucht, sondern in einem bestimmten Dateiformat heruntergeladen und in einer eigens dafür zusammengestellten Datenbank mit Daten desselben Formats zusammengetragen.[45] Im Unterschied zum erwähnten Common Crawl-Datenset, das schlicht einen grossen Teil aller verfügbarer Webseiteninhalte enthält, geht es beim Scraping darum, gezielt spezifische Dateitypen von Webseiten zu extrahieren (oder „runterzukratzen", deshalb „scrapen"). Dabei wird automatisiert der gesamte Inhalt einer Webseite auf vordefinierte Dateninhalte (Textbestandteile, Bilder, E-Mail-Adressen etc.) durchsucht. Die gewünschten Inhalte werden in einem zweiten Schritt in einer Datenbank strukturiert.[46] Mit Web Scraping werden also Inhalte gezielt gesucht, extrahiert, kopiert, gespeichert und in Datenbanken strukturiert, damit sie in der Folge beliebig weiterbearbeitet werden können.[47] Kombiniert mit einer späteren Durchsuchung ebendieser Daten, erweitert das Scraping herkömmliches Crawling um ein weiteres Element.

Diese Methode macht es bspw. möglich, Bilddaten von Facebook oder alle Tweets zu einem bestimmten Thema zu sammeln.[48] Scraping kann aber auch zur Sammlung von Verkaufsangeboten (z.B. mit gefälschten Waren) oder pornographischen Inhalten genutzt werden.[49] Für OSINT ist Scraping ferner dienlich, um online veröffentlichte Bild- und Videoaufnahmen von bestimmten Ereignissen wie Demonstrationen zu sammeln.[50] Bilder werden im Netz aufgespürt und in einem bestimmten, technisch weiterverarbeitbaren Format

---

45 Logos/Brewer/Langos/Westlake, 1.

46 Für eine Übersicht siehe z.B. „WebScraping & OSINT: A Beginners Guide", abrufbar unter <https://medium.com/@investigator515/webscraping-osint-a-beginners-guide-bec9ef686dd>.

47 Krotov/Silva, 2.

48 Vgl. Gibson, 78.

49 Logos et al.

50 Siehe dazu die Beispiele von Rückert, Verbrecherjagd.

heruntergeladen. Die Datenbank der Gesichtserkennungssoftware Clearview bspw. basiert auf über 3 Milliarden Gesichtsbildern, die von Webseiten gescraped wurden.[51]

c) Intelligente Datenweiterberarbeitung

Schliesslich können zur OSINF-Gewinnung spezialisierte Systeme eingesetzt werden, die auf breiter Basis Informationen im Netz suchen, extrahieren und in der Folge mit intelligenten Methoden auswerten. „Intelligent" meint dabei, dass avancierte und i.d.R. KI-gestützte Systeme Anwendung finden, die mit grossen Datenmengen trainiert wurden und in der Lage sind, OSINF aus verschiedensten Quellen zu verknüpfen und in den Datensätzen Muster, Trends oder Inhalte wiederzuerkennen.[52] Bei Suchmaschinen-Recherchen werden bestehende Webseiteninhalte anhand bestimmter Begriffe durchsucht und die Ergebnisse einzeln präsentiert oder – bei generativen Systemen – darauf gestützt neue Inhalte produziert. Beim Web Scraping werden Daten darüber hinaus extrahiert und gespeichert. Die hier als dritte Kategorie angesprochenen intelligenten (respektive noch intelligenteren) Methoden sind darauf ausgerichtet, zuvor erlangte grosse Datenmengen miteinander zu verknüpfen und auszuwerten, um dadurch neue, über die einzelnen Daten hinausgehende „Meta-Informationen" zu erlangen.[53] Die Informationen werden somit nicht bloss beschafft, sondern mit KI-Systemen weiterberarbeitet und aufbereitet. Sie erhalten damit eine neue Datenqualität.

Ein Beispiel einer solchen Datenweiterbearbeitung ist die bereits erwähnte Anwendung PimEyes, die mit Gesichtserkennungstechnologie ausgestattet ist und mit der sich über 900 Millionen gescrapte Gesichtsbilder auf Übereinstimmung mit Bildern einer bestimmten Person durchsuchen lassen.[54] Die Bilder werden biometrisch analysiert und mithilfe von KI ähnliche Gesichter erkannt.[55] Ein weiteres Beispiel sind die Anwendungen von „SocialLinks", die eine ganze Palette an intelligenten Tools anbieten, die riesige Datenmengen aus über 500 offenen Quellen in den sozialen Medien, in Blockchains und im Darknet sammeln und darin Muster oder bestimmte Objekte erkennen. Konkret können damit z.B. Accounts und Posts aus verschiedenen sozialen Medien

---

51 Rezende, 375 ff.

52 Rückert, Verbrecherjagd.

53 Rückert, Online-Streife, 328.

54 Harwell, 63 ff.

55 So die Angaben von PimEyes, abrufbar unter <https://pimeyes.com/en/blog/artificial-intelligence-facial-recognition-and-conspiracy-theories>.

mit KI analysiert und über die verschiedenen Netzwerke hinweg Beziehungen zwischen Nutzerinnen visualisiert werden.[56] Weitere derartige Anwendungen werden nicht kommerziell angeboten, sondern von Behörden eigens entwickelt, wie bspw. der „Dark Web Monitor", ein OSINT-Verzeichnis, das kriminelle Aktivitäten im Darknet erfasst, kategorisiert und Zusammenhänge herstellt.[57]

Kennzeichnend für OSINT-Methoden dieser Kategorie ist, dass grosse Datenmengen aus verschiedenen Quellen verknüpft und weiterbearbeitet werden. Diese Art von OSINT nimmt das Crawling und Scraping ebenso als Ausgangspunkt, unterwirft die Daten aber weiteren Datenbearbeitungsschritten und generiert damit zusätzlichen kriminalistischen Wert.

2. Weitere Aspekte der Differenzierung

Neben der Methode der Datenbeschaffung können auch deren Zweck, die Art der erlangten Daten sowie die zu überwindenden technischen Hürden der weiteren Unterscheidung verschiedener OSINT-Kategorien dienen. Diese Faktoren prägen das kriminalistische Vorgehen und die rechtliche Einordnung gleichermassen.

a) Zweck

Der Zweck der Datenbearbeitung ist entscheidend, um das anwendbare Recht zu bestimmen. Zunächst ist es möglich, dass sich Strafverfolgungsbehörden i.S.e. *Online-Streife* auf Webseiten bewegen und OSINF wahrnehmen, ohne einen im Vorfeld klar umrissenen Ermittlungszweck zu verfolgen.[58] Der Zweck solcher virtueller „Streifenfahrten" besteht in der Beobachtung bestimmter Webseiten zur präventiven Verhinderung oder der Erkennung von Straftaten.[59] Da sie ohne konkreten Anfangsverdacht erfolgen, handelt es sich um dem Polizeirecht unterliegende rein präventiv-polizeiliche Massnahmen. Im Kontrast dazu kann OSINT dazu dienen, zielgerichtet aufgrund einer konkreten Verdachtslage an Informationen zu gelangen. Bei *gezielten Online-Re-*

---

56 Siehe die Übersicht von SocialLinks, abrufbar unter <https://www.maltego.com/transform-hub/social-links-pro/>,

57 Bayerisches Staatsministerium der Justiz, „Ein Jahr Dark Web Monitor", abrufbar unter <https://www.justiz.bayern.de/presse-und-medien/pressemitteilungen/archiv/2021/118.php>.

58 So die Begrifflichkeit bei RÜCKERT, Online-Streife, 306.

59 Zu solchen Beobachtungen im Internet HANSJAKOB, 247.

cherchen liegt der Zweck in der Führung eines Tatnachweises gegenüber tatverdächtigen Personen.[60] Es handelt sich um eine genuin strafprozessuale Massnahme, bei der im Nachgang zu bestimmten, verdachtsauslösenden Ereignissen Informationen im Netz recherchiert werden. Denkbar ist des Weiteren, OSINT für *Online-Rasterfahndungen* zu nutzen, die helfen sollen, den Kreis möglicher Tatverdächtiger überhaupt erst auszumachen oder Spurenansätze zu generieren.[61] Schliesslich kann OSINT zur *Online-Überwachung* von Vorgängen oder Zielpersonen erfolgen.[62] Dabei geht es um die länger andauernde Überwachung von Aktivitäten bestimmter Zielpersonen (z.B. in Webforen,[63] oder auf Social Media). Auch hier handelt es sich nur um eine strafprozessuale Massnahme, wenn die Ermittlung einer konkreten Verdachtslage folgt.

b) Art der Daten

Die Art der bearbeiteten Daten ist ein weiterer massgeblicher Aspekt einer Kategorisierung. Herangezogen werden kann die datenschutzrechtliche Unterscheidung zwischen Daten ohne Personenbezug (Sachdaten), Personendaten, besonders schützenswerten Personendaten und Persönlichkeitsprofilen (Art. 5 lit. a, c und f DSG). Je persönlichkeitsnaher die Daten, desto invasiver die Datenbearbeitung.[64] So ist die Bearbeitung besonders schützenswerter Personendaten i.d.R. mit einem schwerwiegenden Eingriff in Art. 13 Abs. 2 BV verbunden.[65] Dabei ist auch die Sensitivität allfälliger bekanntgegebener Daten zu berücksichtigen. OSINT-Methoden können sich also danach unterscheiden, welche Art von Datenbearbeitungen sie involvieren. Werden nur Sachdaten bearbeitet (wie z.B. bei Suchabfragen zu einem Tatmittel), ist dies grundsätzlich unproblematisch. Davon zu unterscheiden sind Abfragen, die sich auf bestimmte oder bestimmbare Personen beziehen (z.B. Eingabe von E-Mail-Adressen). Schliesslich können die Abfragen persönlichkeitsnahe Informationen betreffen, wobei zu beachten ist, dass Informationen, die Rückschlüsse über eine strafrechtliche Verfolgung zulassen, per se als besonders schützenswert gelten (vgl. Art. 5 lit. c Ziff. 5 DSG). In diese Kategorie fallen auch biometrische Daten (vgl. Art. 5 lit. c Ziff. 4 DSG).

---

60 Siehe Rückert, Online-Streife, 307 zur Gewinnung von Beweisdaten.

61 Rückert, Online-Streife, 307.

62 Rückert, Online-Streife, 308; Cartner/Schweingruber, 992.

63 Cartner/Schweingruber, 992; Rückert, Online-Streife, 308.

64 Müller, 139; Kiener/Kälin/Wyttenbach, § 14 Rz. 56.

65 SGK BV-Schweizer/Striegel, Art. 13 Rz. 91; Kiener/Kälin/Wyttenbach, § 14 Rz. 56.

c) Technische Hürden

Ein weiterer relevanter Gesichtspunkt stellen (technische) Barrieren dar, die für die Informationsgewinnung überwunden werden müssen. Gewisse Informationen im Netz sind nicht über Standardbrowser abrufbar, sondern nur mit spezialisierter Anonymisierungs- und Verschlüsselungsoftware, so z.B. Inhalte im Dark Web, die nur über den TorBrowser zugänglich sind.[66] Davon zu unterscheiden sind Informationen in sozialen Netzwerken, die – nicht immer, aber meistens – nur zugänglich sind, wenn ein Benutzerprofil erstellt oder eine anderweitige Registrierung durchgeführt wird.[67] Dadurch steigt der Aufwand, der betrieben werden muss, um an die Daten zu gelangen. Relevant ist insbesondere, ob mit dem Überwinden von technischen Hürden auf nicht-öffentliche Bereiche der Kommunikation zugegriffen wird. Dies wäre bspw. bei einer Kontaktaufnahme über eine Follower- oder Freundschaftsanfrage der Fall. In solchen Fällen ist, wie erwähnt, nicht mehr von OSINF auszugehen.[68]

3. Synthese

Open Source-Ermittlungen können mit verschiedenen Methoden zu verschiedenen Zwecken zur Erlangung verschiedener Arten von Daten und unter Überwindung unterschiedlicher Hürden betrieben werden. Es existiert eine breite Palette an Vorgehensweisen. OSINT erstreckt sich von einzelnen Google-Recherchen nach Adressangaben über automatisierte Rasterfahndungen basierend auf Social-Media-Posts bis hin zu KI-gestütztem Scraping von Gesichtsbildern. Zwischen diesen OSINT-Varianten liegen bedeutsame Unterschiede. Eine pauschale Würdigung, dass alles, was online aufgefunden werden kann, ohne weiteres auf jede erdenkliche Art weiterbearbeitet werden darf, wäre insofern zweifellos verkürzt.

---

66 Rückert, Online-Streife, 311; der TorBrowser ist jedoch zum (kostenlosen) Download verfügbar unter: <https://www.torproject.org/de/download/>.

67 Cartner/Schweingruber, 991; vgl. Hansjakob, 247.

68 Cartner/Schweingruber, 996.

IV. Notwendigkeit einer gesetzlichen Grundlage

1. Qualifizierung als Grundrechtseingriff

In Anbetracht der Vielfalt der Kategorien drängt sich die Frage auf, wie sich dies auf die grundrechtliche und, darauf aufbauend, strafprozessrechtliche Einordnung der Ermittlungsmethode auswirkt. Zunächst ist zu klären, ob OSINT überhaupt mit Grundrechtseingriffen einhergeht. CARTNER und SCHWEINGRUBER halten fest, dass es sich bei OSINF-Recherchen um Grundrechtseingriffe handeln könne. Da die Informationen öffentlich seien, würden diese Ermittlungen die von Art. 13 Abs. 1 BV geschützte Privatsphäre allerdings nicht betreffen. Art. 13 Abs. 2 BV erachten sie hingegen als berührt, sofern mit OSINT Personendaten beschafft werden.[69] Der auch als Anspruch auf „informationelle Selbstbestimmung" bezeichnete Art. 13 Abs. 2 BV bietet Schutz vor staatlichem Beschaffen, Sammeln, Verbreiten, Aufbewahren oder Weitergeben von Personendaten.[70] Aufgrund der Datenbearbeitung stehen bei Open Source-Ermittlungen mögliche Eingriffe in Art. 13 Abs. 2 BV im Vordergrund und mit ihm der Schutz vor staatlichem Missbrauch persönlicher Daten. Die informationelle Selbstbestimmung ist allerdings Teilgehalt des Grundrechts auf Privatsphäre, Art. 13 Abs. 2 und Abs. 1 sind folglich stets zusammen zu denken. Es ist ferner nicht auszuschliessen, dass die staatliche Kenntnisnahme von Informationen im Netz (zumindest indirekt) Auswirkungen auf die in Art. 16 BV geschützte Meinungsfreiheit hat.[71]

CARTNER und SCHWEINGRUBER nehmen einen Grundrechtseingriff an, wenn eine Bearbeitung von Personendaten erfolgt. Der Eingriff in Art. 13 Abs. 2 BV wiege bei OSINF jedoch „weniger schwer", insbesondere wenn die betroffene Person mit der Veröffentlichung einverstanden war.[72] Ferner handle es sich bei OSINF-Recherchen nicht um Zwangsmassnahmen, da mit OSINT beschaffte Beweismittel nicht mittels den – in Art. 197 ff. StPO spezifisch normierten – Zwangsmassnahmen erhoben werden.[73] Dem ist entgegenzuhalten, dass sich der Zwangsmassnahmencharakter einer Massnahme aus deren Qualifikation

---

69 CARTNER/SCHWEINGRUBER, 992.

70 MÜLLER/SCHEFER, 167; KIENER/KÄLIN/WYTTENBACH, § 14 Rz. 57; BSK BV-EPINEY, Art. 13 Rz. 33.

71 Indirekte Auswirkungen auf die Meinungsfreiheit i.S.v. „chilling effects" könnten angenommen werden, wenn Bürger aufgrund des Wissens um die Präsenz von Behörden im Netz von der Veröffentlichung ihrer Meinungen in Online-Medien abgeschreckt werden, weiterführend dazu BÜCHI/FESTI/LATZER.

72 CARTNER/SCHWEINGRUBER, 993.

73 CARTNER/SCHWEINGRUBER, 990 und 994 ff.

als Grundrechtseingriff ergibt. Jeder Grundrechtseingriff, welcher der strafprozessualen Ermittlung und damit der Beweisführung dient, stellt eine Zwangsmassnahme dar (vgl. Art. 196 StPO), unabhängig von der Intensität des Eingriffes.[74] Die Frage, ob überhaupt ein Grundrechtseingriff und folglich eine Zwangsmassnahme vorliegt, ist von derjenigen nach der Schwere des Grundrechtseingriffes zu trennen. Nachfolgend ist deshalb in einem ersten Schritt zu klären, ob bzw. ab wann OSINT einen Grundrechtseingriff darstellt und wie sich die Einwilligung auf die Qualifikation als Eingriff auswirkt, bevor die Eingriffsschwere der einzelnen Methoden diskutiert wird.

Involviert OSINT die Bearbeitung von Personendaten, berührt dies grundsätzlich den Schutzbereich von Art. 13 Abs. 2 BV und erfordert eine gesetzliche Grundlage (Art. 36 Abs. 1 BV). Aufgrund der öffentlichen Zugänglichkeit der Informationen könnte allerdings argumentiert werden, dass die Veröffentlichung im Internet einer Einwilligung der betroffenen Person gleichkommt.[75] In der Lehre ist strittig, ob eine Einwilligung die Voraussetzung einer gesetzlichen Grundlage nach Art. 36 BV zu ersetzen vermag.[76] Malacrida zufolge kommt eine ausdrückliche Einwilligung einem Grundrechtsverzicht gleich, der eine gesetzliche Grundlage zu substituieren vermag.[77] Andererseits wird angenommen, es bedürfe auch im Falle einer Einwilligung stets einer Rechtsgrundlage, ansonsten würde dies dem Legalitätsprinzip widersprechen.[78] Gemäss Epiney ist von dieser Frage der Einwilligung als Gesetzessurrogat diejenige nach der Eröffnung des Schutzbereichs eines Grundrechts zu unterscheiden. Eine Einwilligung könne abhängig vom betroffenen Grundrecht implizieren, dass der Schutzbereich gar nicht erst berührt ist. Für sie stellt die Frage nach der Einwilligung deshalb eine Frage nach dem Vorhandensein eines Grundrechtseingriffs schlechthin dar.[79] In der Tat lässt sich verfassungsrechtlich diskutieren, ob die Einwilligung eine tatbestandsausschliessende oder rechtfertigende Wirkung entfaltet. Ersteres wäre anzunehmen, wenn die Einwilligung dazu führte, dass der Eingriffscharakter der Massnahme entfällt. Es bedürfte weder einer Gesetzesgrundlage noch einer Rechtfertigung. Ein Grundrechtseingriff läge gar nicht erst vor.[80] Gegen diese Auffassung spricht gemäss van

74 BGE 145 IV 42, E. 4.2, S. 47.

75 Für den Einwilligungscharakter der Veröffentlichung Cartner/Schweingruber, 993; vgl. OFK DSG-Held/Brönimann, Art. 34 Rz. 29.

76 Siehe dazu SGK BV-Schweizer/Krebs, Art. 36 Rz. 30 m.w.H.; Häner, 57 ff.

77 Malacrida, 140 ff.

78 Dazu z.B. Fasnacht, 94; BSK BV-Epiney, Art. 36 Rz. 32.

79 BSK BV-Epiney, Art. 36 N 32.

80 van Spyk, 120; Fasnacht, Fn. 263.

SPYK, dass Grundrechte nicht nur Ausdruck von Individualrechten sind, sondern auch als „Programmsätze" auf die gesamte Rechts- und Staatsordnung ausstrahlen. Als solche würden sie nicht allein der Verfügungsgewalt der Grundrechtsträger unterliegen. Ein rechtfertigungsbedürftiger Grundrechtseingriff sei nur zu verneinen, wenn ausschliesslich das Selbstbestimmungsrecht der Grundrechtsträger betroffen ist.[81] Ähnlich kommt ZIMMERLIN in Bezug auf den Verzicht auf Verfahrensrechte zum Schluss, dass Grundrechte nicht nur individuelle Schutzansprüche darstellen, sondern als Ordnungs- und Gestaltungsprinzipien der Rechtsordnung ebenfalls objektiv-rechtlichen Gehalt aufweisen.[82]

Wird bei OSINT vom Vorliegen einer Einwilligung ausgegangen, könnte demzufolge je nach Auffassung entweder gar nicht erst ein Eingriff in Art. 13 Abs. 2 BV vorliegen oder die Einwilligung könnte als Rechtfertigung in den Grundrechtseingriff gewertet werden. Für ersteres spricht, dass das meist (aber nicht ohne Kritik[83]) als informationelle Selbstbestimmung bezeichnete Grundrecht gerade darin besteht, über persönliche Informationen frei verfügen zu können. Entscheiden Grundrechtsträger aus freien Stücken, Informationen preiszugeben, machen sie von eben diesem Recht Gebrauch.[84] Gegen diese Auffassung spricht, dass der in Art. 13 Abs. 2 BV festgehaltene „Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten" dahingehend auszulegen ist, dass er den Staat mitunter programmatisch dazu auffordert, persönliche Daten zurückhaltend und nicht missbräuchlich zu bearbeiten. Es handelt sich um eine verfassungsrechtliche Verankerung des Datenschutzes per se.[85] Daraus leiten sich Pflichten betreffend die Datensicherheit, datenschutzfreundliche Voreinstellungen sowie die automatisierte Datenbearbeitung ab, womit der Norm nicht ausschliesslich individualrechtlicher Charakter zukommt. Für diese Einordnung spricht ferner, dass Art. 34 Abs. 4 lit. b DSG vorsieht, dass auf eine gesetzliche Grundlage verzichtet werden kann, wenn die betroffene Person in die staatliche Datenbearbeitung eingewilligt oder ihre Personendaten allgemein zugänglich gemacht hat, ohne eine Bearbeitung ausdrücklich zu untersagen. Die Einwilligung in Kombination mit dieser Rechtsgrundlage legitimiert in diesen Fällen den Grundrechtseingriff.[86] Die Norm führt die

---

81 VAN SPYK, 121 f.

82 ZIMMERLIN, Rz. 487 f.

83 Siehe z.B. GÄCHTER/WERDER, 91 ff.; FLÜCKIGER, 853 ff.

84 In diesem Sinne Onlinekommentar CCC-GRAF, Art. 32 Rz. 36.

85 Vgl. OFK BV-BIAGGINI, Art. 13 Rz. 11 ff.

86 Vgl. OFK DSG-HELD/BRÖNNIMANN, Art. 34, Rz. 27 mit Verweis auf GLASS, 235.

Einwilligung als Surrogat einer gesetzlichen Bearbeitungsgrundlage ein. Der Gesetzgeber ging bei deren Schaffung also offenkundig davon aus, dass der Grundrechtseingriff trotzdem erfolgt und einer Rechtsgrundlage bedarf.

In der strafprozessrechtlichen Literatur beschäftigt diese Frage in analogem Sinne und wird anhand der Einwilligung bei Hausdurchsuchungen diskutiert, wobei verschiedene Lehrmeinungen vertreten werden.[87] Einerseits wird angenommen, dass bei Vorliegen einer Einwilligung gar keine Zwangsmassnahme mehr vorliegt, weshalb die strafprozessualen Bestimmungen keine Anwendung fänden.[88] Andererseits wird vertreten – und vom Bundesgericht gestützt –, dass eine Hausdurchsuchung unabhängig einer Einwilligung stets einen Grundrechtseingriff und damit eine Zwangsmassnahme darstellt.[89] Die Einwilligung wird insofern als Grundrechtsverzicht gewertet, ihr zugleich aber keine eingriffsausschliessende Wirkung zuerkannt.[90]

Somit kann festgehalten werden, dass Open Source-Ermittlungen grundsätzlich als Grundrechtseingriffe und konsequenterweise als (der Beweissicherung dienende) Zwangsmassnahmen zu qualifizieren sind,[91] sofern sie die Bearbeitung von Personendaten betreffen. Die Einwilligung schliesst den Grundrechtseingriff nicht aus.[92]

Es stellt sich aber sowohl im Verfassungsrecht[93] als auch im Strafprozessrecht[94] die Frage, ob die Einwilligung die gesetzliche Grundlage ersetzen kann. Die Konsequenzen der Einwilligung sind im Datenschutzrecht in Art. 34 DSG, wie erwähnt, explizit gesetzlich festgemacht. Im Falle einer Hausdurchsuchung ist dem Bundesgericht zufolge bei einer Einwilligung bloss deshalb kein Hausdurchsuchungsbefehl erforderlich, da dies in Art. 244 Abs. 1 StPO gesetz-

---

87 Zhuoli, 298; BSK StPO 2010-Gfeller/Oswald, Art. 249 Rz. 6 ff.; im Kontext einer Videoüberwachung hatte das Bundesgericht die Frage noch offengelassen, BGE 145 IV 42 E. 4.4 S. 47.

88 Zhuoli, 298 mit Verweis auf BSK StPO 2010-Gfeller/Oswald, Art. 249 Rz. 6 ff.; BSK StPO 2010-Gfeller, Art. 241 Rz. 4.

89 Urteil des Bundesgerichts 6B_900/2015 vom 29. Januar 2016, E. 1.4.3; Zhuoli, 298 mit Verweis auf BSK StPO 2014-Gfeller/Oswald, Art. 249 N 1c.

90 Montero/Simon, 100.

91 Vgl. BGE 145 IV 42 E. 3 und 4.2 S. 47.

92 Dafür spricht ferner, dass strafprozessuale Massnahmen auch bei Vorliegen einer Einwilligung an einen Tatverdacht geknüpft sind. Der Grundrechtsträger kann mit seiner Einwilligung dieses prozessuale Erfordernis nicht entfallen lassen.

93 Siehe zur Debatte SGK BV-Schweizer/Krebs, Art. 36 Rz. 30.

94 Montero/Simon, 100 m.w.H.

lich verankert ist.[95] Auch hier führt also erst das Gesetz die Einwilligung als Rechtfertigung ein. Da die StPO den Umgang mit OSINF nicht gesetzlich reguliert, stellt sich die Frage, ob eine Einwilligung dennoch als Gesetzessurrogat ausreichen würde. In der öffentlich-rechtlichen Literatur wird dies vereinzelt davon abhängig gemacht, ob es sich um einen schweren Grundrechtseingriff handelt.[96] Dem wird richtigerweise entgegengehalten, dass auch für „gewöhnliche" Grundrechtseingriffe stets eine gesetzliche Grundlage notwendig sei.[97] Es handelt sich bei personenbezogener OSINT um einen Grundrechtseingriff, da Art. 13 Abs. 2 BV als Programmsatz staatliches Handeln reguliert und nicht nur der alleinigen Disposition der Grundrechtsträger unterliegt. Das in Art. 2 Abs. 2 StPO für das Strafprozessrecht verankerte Legalitätsprinzip macht es erforderlich, staatliches Handeln in vom Gesetz vorgesehene Formen zu giessen. Die Einwilligung vermag es für sich allein nicht, diesen Anspruch aufzuheben.

Die Anforderungen an die Bestimmtheit der Normen sind allerdings deutlich tiefer bei leichten Grundrechtseingriffen. Wird angenommen, dass bei Veröffentlichung von Daten durch die betroffene Person nur ein minimalinvasiver Eingriff vorliegt, könnte es folglich ausreichen, dass das Strafprozessrecht in seiner Gesamtheit den Strafverfolgungsbehörden die Ermittlungsarbeit als Aufgabe überträgt, staatliches Handeln hier also zweckgerichtet erfolgt. Die Rechtsgrundlage wäre in den allgemeinen Zweckbestimmungen des Strafprozessrechts zu erblicken, welche die Aufklärung von Straftaten festschreiben und staatliches Handeln binden. Es bedürfte, dieser Annahme folgend, keiner präzis normierten gesetzlichen Grundlage für minimalinvasive OSINT-Massnahmen. Die Einwilligung würde die Anforderung an das Bestehen gesetzlicher Rahmenbedingungen dennoch nicht gänzlich entfallen lassen. Sie rechtfertigt den Grundrechtseingriff nicht für sich allein, vermag dessen Invasivität aber zu senken. Das Vorhandensein der Einwilligung liesse es zu, tiefe Anforderungen an die Bestimmtheit der Norm zu stellen: einerseits aufgrund der minimalen Invasivität, andererseits aufgrund der tiefen Ansprüche an die Voraussehbarkeit staatlichen Handelns im Falle eben dieser Einwilligung. Auch allgemeine gesetzliche Rahmenordnungen staatlichen Handelns könnten demzufolge bei solchen Konstellationen als ausreichend erachtet werden. Sobald

---

95 BGer 6B_900/2015, E. 1.4.3.

96 Siehe z.B. Eicker/Mango-Meier, 664 f.; SGK BV-Schweizer/Striegel, Art. 13 Rz. 128.

97 BSK BV-Epiney, Art. 36 Rz. 32.

es sich allerdings nicht mehr um minimalinvasive Massnahmen handelt oder das Vorliegen einer Einwilligung nicht ohne weiteres angenommen werden kann, stösst diese Argumentation an rechtstaatliche Grenzen.

Zur Qualifikation als Grundrechtseingriff lässt sich insgesamt festhalten, dass (1.) OSINT den Schutzbereich von Art. 13 BV berührt. Dabei wirkt sich (2.) die Einwilligung nicht tatbestandsausschliessend aus, weshalb ein Grundrechtseingriff bzw. – bei OSINT zu Ermittlungszwecken – eine Zwangsmassnahme vorliegt. Grundrechtseingriffe bedürfen (3.) auch bei Vorliegen einer Einwilligung einer Rechtsgrundlage; die Einwilligung ist kein Gesetzessurrogat, sondern verringert höchstens die Anforderungen an die Bestimmtheit der Grundlage.

2. Reichweite der Einwilligung

Das Vorausgegangene folgte der Annahme, dass bei OSINF, d.h. bei bereits öffentlich zugänglichen Informationen, vom Vorliegen einer Einwilligung der berechtigten Person ausgegangen werden kann. Dies ist nicht ohne weiteres zutreffend. Die Voraussetzungen einer gültigen Einwilligung werden in der konkludenten oder ausdrücklichen Kundgabe der Einwilligung, d.h. der eigentlichen Einwilligungserklärung, sowie in der dieser vorausgehenden freien Willensbildung erblickt.[98] Bei strafprozessualen Zwangsmassnahmen nimmt das Bundesgericht an, dass eine Einwilligung ausdrücklich zu erfolgen hat.[99]

Bei der Bearbeitung von OSINF durch Strafverfolgungsbehörden kann vom Vorliegen einer Einwilligung ausgegangen werden, wenn die betroffene Person selbst Informationen im Wissen um eine mögliche Einsichtnahme durch Behörden preisgibt.[100] Darauf ist zu schliessen, wenn in Anbetracht der gesamten Umstände naheliegt, dass die Person sowohl die Veröffentlichung für einen unbestimmten Kreis von Personen als auch eine mögliche Weiterverwendung im Rahmen behördlicher Verfahren zumindest in Kauf nahm. In der Regel ist dies der Fall, wenn Informationen ohne jegliche technischen Hürden durch die Person selbst veröffentlicht wurden (z.B. auf einem öffentlichen Social Media-Profil). Unterliegen die Informationen Zugangsschranken, kann demgegenüber

98 Ausführlich VAN SPYK, 107 ff.

99 Urteil des Bundesgerichts 6B_996/2016 vom 11. April 2017, E. 3.4; dazu EICKER/MANGO-MEIER, 661.

100 Dazu auch BAUER, 116 ff.

nicht mehr ohne weitere Prüfung von einer Einwilligung ausgegangen werden. Im Umgang mit besonders schützenswerten Personendaten ist zudem auf eine ausdrückliche Einwilligung abzustellen (vgl. Art. 6 Abs. 7 lit. a DSG).

In der Praxis dürfte sich die Problematik ergeben, dass im Moment der Suchabfrage allenfalls noch unbekannt ist, welche Personendaten überhaupt beschafft werden. Hier ist die Absicht der Ermittlung ausschlaggebend. Impliziert die Methode bereits die Absicht, auf nicht ohne weiteres zugängliche Daten zu stossen, kann nicht auf eine konkludente Einwilligung verwiesen werden.

Ferner stellt sich die Frage, wie weit die Einwilligung greift. Veröffentlichen Grundrechtsträger persönliche Daten im Internet, willigen sie zunächst einmal in diese Veröffentlichung ein. Dies impliziert zwar die Einwilligung in die Kenntnisnahme durch andere Internetnutzerinnen, nicht jedoch eine behördliche Weiterverwendung der Personendaten. Das Aufschalten eines Profilbilds auf Facebook ist nicht dahingehend zu interpretieren, dass in das Scraping der Bilder oder deren biometrische Vermessung zu strafprozessualen Zwecken eingewilligt wird. Dasselbe dürfte für intelligente Methoden, mit denen Daten aus verschiedenen Quellen verknüpft und zu neuen Informationen in Form von personenbezogenen Profilen weiterberarbeitet werden, gelten. Folglich ist im Einzelfall zu prüfen, ob die Einwilligung tatsächlich die gesamte OSINT-Massnahme abzudecken vermag.

Schliesslich ist anzumerken, dass viele Informationen im Internet nicht durch die datenberechtigte Person selbst zur Verfügung gestellt werden. Auch deshalb bietet sich Zurückhaltung bei der Annahme einer Einwilligung an.

3. Eingriffsschwere

Grundrechtseingriffe können mehr oder weniger invasiv ausfallen.[101] Verfassungsmässig besteht zwar für leichte Eingriffe keine Ausnahme vom Erfordernis einer gesetzlichen Grundlage,[102] und auch die StPO unterscheidet nicht zwischen „leichten“ und „schweren“ Zwangsmassnahmen.[103] Dennoch ist die Invasivität relevant, weil bei schwerwiegenden Einschränkungen höhere Anforderungen an Normstufe und Normdichte gestellt sind: je schwerer der Ein-

101 BSK BV-Epiney, Art. 36 Rz. 21.
102 BSK BV-Epiney, Art. 36 Rz. 32.
103 Vgl. BGE 145 IV 42, E. 4.2, S. 47.

griff, desto klarer und präziser muss die gesetzliche Grundlage sein.[104] Darüber hinaus bedürfen eingriffsintensivere Zwangsmassnahmen höhere Tatverdachtsgrade.[105]

Für die Beurteilung der Eingriffsschwere gelten keine allgemeinen, abstrakten Kriterien.[106] Indikatoren für schwerwiegende Eingriffe in Art. 13 Abs. 2 BV sind jedoch u.a. die grosse Persönlichkeitsnähe der Informationen,[107] die Bearbeitung besonders schützenswerter Daten,[108] die Kombination von Daten mit verschiedenen Datenquellen,[109] oder eine grosse Streubreite von Informationsbeschaffungsmassnahmen, welche (im strafprozessualen Kontext) auch eine grosse Anzahl nicht tatverdächtiger Personen umfasst.[110] Für einen leichten Eingriff hingegen spricht, wenn sich die Datenbearbeitung auf einzelne Informationen beschränkt, an welchen die betroffene Person mit der eigenständigen Veröffentlichung ihre Vertraulichkeitserwartung aufgegeben hat.[111]

Wie festgehalten wurde, handelt es sich bei Open Source-Ermittlungen um Grundrechtseingriffe, bei denen – im Falle von leichten Eingriffen – die Einwilligung eine weitgehend (wenn auch nicht vollumfängliche) legitimierende Wirkung entfaltet respektive den Grundrechtseingriff weiter schmälert. Der Schutz vor missbräuchlicher staatlicher Datenbearbeitung wird zwar dennoch berührt und eine gesetzliche Grundlage bleibt erforderlich, die Einwilligung reduziert die Eingriffsschwere der Massnahme allerdings drastisch.[112] Die Rechtsgrundlage könnte, wie bereits angedeutet, in den allgemeinen strafprozessualen Bestimmungen bzw. den prozessrechtlichen Rahmenbedingungen erblickt werden. Die allgemeine Zweckbindung staatlicher Tätigkeit würde demnach dem Legalitätsprinzip Genüge tun und den programmatischen Charakter des Grundrechtsschutzes abdecken, während der individualrechtliche Charakter von der selbstbestimmten Einwilligung gedeckt wäre. Dies vermag für schwere Grundrechtseingriffe hingegen nicht zu überzeugen. Es bedingt

---

104 BSK BV-Epiney, Art. 36 Rz. 36; SGK BV-Schweizer/Krebs, Art. 36 N 23.

105 BSK StGB 2023-Weber, Art. 197 N 8.

106 BSK BV-Epiney, Art. 36 N 21; Müller, 136.

107 Müller/Schefer, 170; SGK BV-Schweizer/Striegel, Art 13 Rz. 122; Kiener/Kälin/Wyttenbach, § 14 Rz. 56.

108 Art. 34 Abs. 2 lit. a DSG.

109 So insbesondere das BGer in Bezug auf die AFV BGE 146 I 11 E. 3.1.2 S. 14.

110 Dazu BGE 146 I 11 E. 3.1.2 S. 14; Müller, 137 ff.; ebenfalls die Kriterien von Rückert, Online-Streife, 320 ff.

111 Rückert, Online-Streife, 323 f.

112 Ähnlich geht auch Rückert für das Deutsche Recht davon aus, dass die eigene Veröffentlichung der Daten die Eingriffsintensität massgeblich reduziert, Rückert, Digitale Daten, 269.

zudem das Bestehen einer Einwilligung, da erst diese die Invasivität der Massnahme abschwächt und die Bestimmtheitsanforderungen an die Rechtsgrundlage senkt. Wie soeben aufgezeigt, kann jedoch nicht bei allen Informationen im Internet davon ausgegangen werden, dass eine solche Einwilligung hinsichtlich aller möglichen Weiterbearbeitungsmassnahmen vorliegt.

Wie im ersten Teil der Abhandlung aufgezeigt, lässt sich OSINT in verschiedener Hinsicht kategorisieren. So konnten Web Crawling, Web Scraping und intelligentere Datenweiterberarbeitungen ebenso wie verschiedene Datenkategorien, Bearbeitungszwecke und technische Hürden differenziert werden. Pauschale Aussagen halten kaum Stand. Trotzdem lässt sich als Ausgangspunkt festhalten, dass schlichtes und generatives Web Crawling öffentlich verfügbarer Personendaten i.d.R. als leichte Eingriffe zu qualifizieren sind. Da die Daten ohne weiteres auffindbar sind und nur beschafft, nicht jedoch qualifiziert weiterbearbeitet werden, kann auf eine mutmassliche konkludente Einwilligung geschlossen werden. Art. 13 Abs. 2 BV ist dann kaum mehr berührt. Web Scraping hingegen, welches das Extrahieren von Daten involviert, kann zwar im Falle einfacher Personendaten nach wie vor als leichter Eingriff qualifiziert werden, hier ist jedoch ohne konkrete gegenteilige Anhaltspunkte nicht mehr von einer weitgehenden Rechtfertigung durch Einwilligung auszugehen. Gleiches gilt für intelligente Weiterberarbeitungen.

Von einem schweren Grundrechtseingriff ist hingegen bei der Bearbeitung besonders schützenswerter Personendaten oder Persönlichkeitsprofilen auszugehen. OSINT-Methoden, welche die biometrische Bearbeitung von Bildmaterial involvieren, automatisiert soziale Beziehungen auswerten oder das Online-Bewegungsverhalten von Nutzerinnen systematisch erfassen, fallen in diese Kategorie. Ebenso sind automatisierte Online-Rasterfahndungen oder Online-Überwachungen mit grosser Streubreite als invasive Massnahmen zu erachten. Die Notwendigkeit, technische Hürden überwinden zu müssen, spricht schliesslich gegen das Vorliegen einer Einwilligung.

4. Synthese

Die breite Palette an OSINT-Kategorien divergiert nach Eingriffsschwere und liefert zugleich Anhaltspunkte für das Vorliegen einer Einwilligung. Es können drei Kategorien unterschieden werden: (1.) Massnahmen, die leichte Eingriffe darstellen und für die eine (mutmassliche) Einwilligung vorliegt, (2.) Massnahmen, die leichte Eingriffe darstellen und die Reichweite der Einwilligung (mutmasslich) übersteigen, und (3.) Massnahmen, die schwere Eingriffe darstellen.

Mit Blick auf die Anforderungen an die Gesetzesgrundlage wurde ausgeführt, dass die Einwilligung grundsätzlich weder den Grundrechtseingriff noch das Erfordernis einer gesetzlichen Grundlage entfallen lässt (Art. 36 Abs. 1 BV). Liegen minimalinvasive Eingriffe vor, können gesetzliche Leitplanken i.S. allgemeiner Zweckbestimmungen, wie sie sich in der Strafprozessordnung als Ganzes finden, ausreichen. Liegt keine Einwilligung vor, steigen die Anforderungen an die gesetzliche Grundlage. Sie hat hinreichend bestimmt zu sein, sodass für die einzelne Person erkennbar ist, unter welchen Voraussetzungen eine Grundrechtseinschränkung erfolgt.[113]

Die unterschiedlichen OSINT-Massnahmen lassen sich nicht pauschal unter eine der drei Eingriffskategorien subsumieren. Sie sind allerdings mehr oder weniger invasiv und deuten auf das Vorliegen oder die Abwesenheit einer mutmasslichen Einwilligung hin. Betreffend die *Methode* steigt die Eingriffsschwere und sinkt die Plausibilität der Einwilligung vom Web Crawling über das Web Scraping bis hin zur intelligenten Datenweiterverarbeitung. Aber auch beim *Zweck* (gezielte Recherche, Rasterfahndung, Überwachung), bei der Art der Daten (Sachdaten, Personendaten, besonders schützenswerte Personendaten und Profile) sowie bei den *technischen Hürden* (keine, Registrierung oder Benutzerprofil, spezialisierte Software) deuten die verschiedenen Kategorien eine höhere Grundrechtsinvasivität an. Im Einzelfall ist die Massnahme einer genaueren Prüfung zu unterziehen. Klar wird aus der bisherigen Analyse jedenfalls, dass OSINT einerseits stets grundrechtsrelevant ist und andererseits bei gewissen OSINT-Methoden nicht ohne weiteres auf eine spezifische Rechtsgrundlage verzichtet werden kann.

V. Rechtmässigkeit

1. Ermittlungsgeneralklausel

OSINT berührt den Schutzbereich von Art. 13 Abs. 2 BV. Verfahrenshandlungen der Strafverfolgungsbehörden, welche für die Betroffenen mit Grundrechtseingriffen einhergehen und der Sicherung von Beweisen, der Anwesenheit von Verfahrensbeteiligten oder der Entscheidvollstreckung dienen, gelten als strafprozessuale Zwangsmassnahmen (Art. 196 lit. a–c StPO).[114] Konstituierend für den Begriff ist einzig die Qualifikation als Grundrechtseingriff sowie der

113 Zuletzt BGE 147 I 478, E. 3.1.2, S. 484 f.

114 SK StPO-Zimmerlin, Art. 196 Rz. 6; BSK StPO 2023-Weber, Art. 196 Rz. 4; Maeder/Stadler, 399.

Zweck dieses Eingriffs. Auf die Intensität des Grundrechtseingriffs kommt es hingegen nicht an.[115] Art. 197 Abs. 1 lit. a StPO normiert ausdrücklich, dass jede Zwangsmassnahme gesetzlich vorzusehen ist, wobei die StPO nicht zwischen schweren und leichten Zwangsmassnahmen unterscheidet.[116] Es besteht ein numerus clausus an Zwangsmassnahmen, weshalb gesetzlich nicht vorgesehene Zwangsmassnahmen unzulässig sind.[117] Ergänzendes Verordnungsrecht für leichte Zwangsmassnahmen gibt es nicht.

Für denjenigen Umgang mit OSINF, der als minimalinvasiver Eingriff zu qualifizieren ist und bei dem eine Einwilligung angenommen werden darf, sind keine hohen Anforderungen an die Bestimmtheit der gesetzlichen Grundlage zu stellen. Die strafprozessuale Gesamtordnung kann bei minimalinvasiven Eingriffen dem Legalitätsprinzip Genüge tun. In Anbetracht des allgemeinen Gesetzeserfordernisses bei Zwangsmassnahmen ist allerdings bereits diese Argumentation nicht unproblematisch. Diese sehr tiefen Anforderungen an die Bestimmtheit können deshalb sicherlich nur überzeugen, wo die Einwilligung den Grundrechtseingriff bereits weitgehend rechtfertigt, die Rechtsgrundlage also nur noch den Zweck staatlichen Handelns vorzugeben hat.

In Ermangelung spezifischer OSINT-Bestimmungen stellt sich nun die Frage, wie bei Vorgehensweisen zu verfahren ist, die von einer Einwilligung nicht mehr gedeckt sind, aber trotzdem noch als leicht zu qualifizieren sind. Auch hier könnte versucht werden, zur Rechtfertigung eine vergleichsweise unbestimmte Grundlage heranzuziehen. Infrage kommt mitunter die Annahme von „Ermittlungsgeneralklauseln", wie sie im Deutschen Strafprozessrecht bestehen (§§ 161 und 163 DE-StPO). Die Diskussion zur Rechtmässigkeit von OSINT dreht sich in Deutschland im Wesentlichen um die Reichweite der Ermittlungsgeneralklauseln, welche die Staatsanwaltschaft und Polizeibehörden ermächtigen, zum Zweck der Erforschung von Straftaten Ermittlungen jeder Art vorzunehmen, soweit nicht andere gesetzliche Vorschriften die Befugnisse besonders regeln (§ 161 Abs. 1 Satz 1 DE-StPO für die Staatsanwaltschaft, § 163 Abs. 1 Satz 1 DE-StPO für die Polizei). §§ 161 und 163 DE-StPO ermächtigen die Behörden zur Durchführung grundrechtsrelevanter Massnahmen von geringer Eingriffstiefe, für die es noch keiner spezifischen Gesetzesgrundlagen in höherer Bestimmtheit bedarf.[118] Leicht wiegende Massnahmen wie gezielte

---

115 BGE 145 IV 42 E. 4.2 S. 47; BSK StPO 2023-Weber, Art. 196 Rz. 8; Maeder/Stadler, 399.

116 Vgl. BGE 145 IV 42 E. 4.2 S. 47.

117 Oberholzer, Rz. 1124; BSK StPO 2023-Weber, Art. 197 Rz. 4.

118 MüKO StPO-Kölbel, § 161 Rz. 6 f.; KK StPO-Weingarten, § 161 Rz. 1; BeckOK StPO-Sackreuther, § 161 Rz. 1.

OSINT-Recherchen über Standardsuchmaschinen lassen sich gemäss h.L. auf §§ 161 und 163 ff. DE-StPO stützen.[119] Invasivere Massnahmen wie eine Online-Rasterfahndung können jedoch nicht mehr auf die Ermittlungsgeneralklauseln gestützt werden.[120] Im deutschen Strafprozessrecht bestehen mit den Ermittlungsgeneralklauseln also allgemeine gesetzliche Grundlagen zur Rechtfertigung von „leichten" Massnahmen.[121]

Fraglich ist, ob das schweizerische Strafprozessrecht ebenfalls über derartige Generalklauseln verfügt. Mit Art. 306 StPO existiert eine allgemeine Bestimmung, welche die Aufgaben der Polizei im Strafverfahren regelt, Ziel und Zweck des Ermittlungsverfahrens normiert und die polizeilichen Ermittlungshandlungen summarisch aufzählt. Art. 306 Abs. 3 StPO hält allerdings fest, dass sich die Polizei an die Vorschriften über die Untersuchung, Beweismittel und Zwangsmassnahmen zu richten hat. Ähnlich ist in Art. 308 Abs. 1 StPO festgehalten, dass die Staatsanwaltschaft in der Untersuchung den Sachverhalt so weit abzuklären hat, dass sie das Vorverfahren abschliessen kann. Gallela und Rhyner sehen in Art. 306 StPO eine allgemeine Ermittlungsklausel für nicht speziell geregelte Ermittlungsmassnahmen, soweit diese nicht oder nur geringfügig in Grundrechte eingreifen und nicht als Zwangsmassnahmen zu qualifizieren sind.[122] Dieser Argumentation kann nur bedingt gefolgt werden, handelt es sich doch auch bei nicht schwerwiegenden Eingriffen um Zwangsmassnahmen. Wie bereits dargelegt, erachtet das Bundesgericht die Schwere der Massnahme oder die Ausübung von Zwang nicht als konstitutiv für Zwangsmassnahmen.[123] Es qualifiziert z.B. die erkennungsdienstliche Erfassung (Art. 260 ff. StPO) als leichten Eingriff und dennoch als Zwangsmassnahme.[124]

Im Vergleich zu den §§ 161 und 163 ff. DE-StPO handelt es sich bei Art. 306 StPO um eine beispielhafte Umschreibung der polizeilichen Kompetenzen im Ermittlungsverfahren, nicht aber um eine eigentliche Befugnisnorm zur Rechtfertigung leichter Ermittlungsmassnahmen. Art. 306 StPO befugt die Polizei nicht zur Durchführung von Massnahmen, die nur geringfügig in grundrechtlich geschützte Positionen eingreifen. Im Unterschied zum deutschen

119 Rückert, Online-Streife, 328; MüKO StPO-Kölbel, § 161 Rz. 11; Sieber/Brodowski, Rn. 42.

120 Rückert, Online-Streife, 332; Sieber/Brodowski, Rn. 43.

121 Dazu KK StPO-Weingarten § 161 Rz. 1; MüKO StPO-Kölbel, § 161 N 6.

122 BSK StPO 2023-Galella/Rhyner, Art. 306 Rz. 19a.

123 BGE 145 IV 42 E. 4.2 S. 47.

124 BGE 145 IV 263 E. 3.4 S. 267; BGE 144 IV 127 E. 2.1 S. 133; Urteil des Bundesgerichts 1B_285/2020 vom 22. April 2021, E. 2.2.

Strafprozessrecht, das Ermittlungshandlungen nicht in einem abschliessenden Zwangsmassnahmenkatalog regelt, geht die schweizerische StPO von der Grundkonzeption aus, dass Zwangsmassnahmen gesetzlich vorzusehen sind und erlässt einen entsprechenden Katalog in den Art. 201 ff. StPO. Dies gilt auch für nicht schwerwiegende Massnahmen. Da Art. 306 Abs. 3 StPO selbst die Bestimmungen über Zwangsmassnahmen vorbehält, ist gesetzessystematisch schwerlich zu argumentieren, dass es sich bei Art. 306 StPO um die eine Generalklausel handelt, die jegliche leichte Grundrechtseingriffe zu legitimieren vermag. Nicht zuletzt bliebe die Frage offen, warum für polizeiliche Massnahmen eine solche bestehen sollte, nicht aber für Massnahmen der Staatsanwaltschaft. Im Übrigen kann auch die „Beweisverwertungsgeneralklausel" von Art. 139 StPO nicht zur Rechtfertigung neuer Zwangsmassnahmen herangezogen werden.[125]

Eine Ermittlungsgeneralklausel lässt sich in der StPO nicht identifizieren. Dennoch erlässt die StPO die Rahmenbedingungen strafprozessualen Handelns. Sie gibt dem Wirken der Strafverfolgungsbehörden einen Rahmen vor und bindet es an einen konkreten Zweck. Eingriffe müssen grundsätzlich auch innerhalb dieser Gesamtordnung auf einer spezifischen Rechtsgrundlage gründen. Das gilt auch für leichte Zwangsmassnahmen. Es ist allerdings zu vertreten, im Bereich speziell leichter Zwangsmassnahmen die Gesamtordnung als gesetzliche Grundlage im Sinne eines „Notankers" heranzuziehen. In Ermangelung von Generalklauseln kann der Beizug dieses Notankers in Konstellationen gerechtfertigt sein, in denen es für Bürger auch ohne bestimmtere Normierung ausreichend vorhersehbar ist, dass entsprechende Verfahrenshandlungen erfolgen. Bei mit Einwilligung veröffentlichten Informationen dürfte dies der Fall sein. Überzeugender wäre es aber zweifellos – um dies bereits an dieser Stelle zu betonen –, auch derartige minimalinvasive Grundrechtseingriffe expliziter vorzusehen. Insofern kann die StPO in ihrer Gesamtheit als Generalklausel für besonders leichte und durch eine Einwilligung abgedeckte Eingriffe fungieren. Liegt keine Einwilligung vor, ist diese Argumentation allerdings auch für leichte Zwangsmassnahmen kaum zu vertreten.

---

125 Dass das BStGer im Urteil vom 27. November 2020 (SK.2020.7), E. 1.6.1 der Beschaffung von OSINF den Zwangsmassnahmencharakter abspricht und diese Informationen als notorisch i.S.v. Art. 139 Abs. 2 StPO qualifiziert, überzeugt nicht. Das BGer hat zu Informationen aus dem Online-Wörterbuch „Wiktionary" festgehalten, dass als allgemein bekannte Tatsachen i.S.v. Art. 139 Abs. 2 StPO nicht sämtliche im Internet auffindbare Informationen gelten, sondern nur solche aus verlässlichen Quellen, denen einen offiziellen Anstrich anhaftet (BGE 143 IV 380 E. 1.2 S. 385). Dies kann bei OSINF in aller Regel gerade nicht angenommen werden.

2. Übereinkommen über die Cyberkriminalität

Kann nicht bei allen OSINT-Kategorien auf eine explizite gesetzliche Verankerung verzichtet werden, stellt sich die Frage, wo eine solche zu finden ist. Infrage kommt die Convention on Cybercrime (CCC), die sich mit Cyberkriminalität und der Beschaffung von Daten befasst. Für Datenbeschaffungen im Rahmen strafprozessualer Ermittlungen relevant sind Art. 31–34 CCC, die hinsichtlich des Rechtshilfeverhältnisses self-executing sind, d.h. direkt anwendbares Recht für Ermittlungshandlungen in anderen Staaten erlassen.[126] Art. 32 CCC regelt dabei den grenzüberschreitenden Zugriff auf Daten. Er legt für die Vertragsstaaten verbindlich fest, unter welchen Umständen Ermittlungsbehörden direkt (d.h. ohne förmliches Rechtshilfeverfahren) auf im Ausland befindliche Daten zugreifen dürfen.[127]

Art. 32 lit. a CCC enthält eine spezifische Bestimmung für den Zugriff auf öffentlich zugängliche Daten: Eine Vertragspartei darf ohne die Genehmigung einer anderen Vertragspartei auf öffentlich zugängliche gespeicherte Computerdaten (offene Quellen) zugreifen, unabhängig davon, wo sich die Daten geographisch befinden. Damit wird festgehalten, dass Strafverfolgungsbehörden ohne Rechtshilfeersuchen auf OSINF zugreifen dürfen.[128] Art. 32 lit. a CCC stellt somit eine konventionsrechtliche Grundlage für den grenzüberschreitenden Abruf von OSINF dar und normiert einen Verzicht auf die sonst üblichen Prozesse der förmlichen Rechtshilfe.[129] Graf vertritt die Meinung, dass die Bestimmung bloss deklaratorischer Natur ist, da mangels Zwangsausübung die Eingriffsqualität von OSINF-Abfragen ohnehin zu verneinen sei.[130] Dem ist, wie bereits dargelegt, zu widersprechen, geht OSINT doch mit einem Grundrechtseingriff einher. Fraglich bleibt allerdings, inwieweit Art. 32 lit. a CCC auch im innerstaatlichen Verhältnis als gesetzliche Grundlage für Open Source-Abfragen taugt.

Die Norm dient dazu, bestimmte Konstellationen des grenzüberschreitenden Zugriffs, die auch bereits vor Erlass der Konvention praktiziert wurden und bezüglich derer alle Vertragsstaaten der Auffassung waren, dass einseitige

---

126 Onlinekommentar CCC-Graf, Art. 32 Rz. 17; Graf, Strafverfolgung 2.0, Rz. 35; vgl. Explanatory Report to the convention on Cyberrime, abrufbar unter <https://rm.coe.int/16800cce5b>, Rz. 293 und Rz. 255.

127 Graf, Jusletter, Rz. 35; Onlinekommentar CCC-Graf, Art. 32 Rz. 4.

128 MüKO StPO-Rückert, § 100a Rz. 45; Onlinekommentar CCC-Graf, Art. 32 Rz. 4.

129 Vgl. Walder, 542.

130 Graf, Strafverfolgung 2.0, Rz. 29; Onlinekommentar CCC-Graf, Art. 32 Rz. 35.

Vorgehensweise akzeptierbar sei, auf ein geschriebenes rechtliches Fundament zu stellen.[131] Inländische Strafverfolgungsbehörden können sich unmittelbar auf Art. 32 CCC stützen, um Beweiserhebungen im Ausland zu legitimieren und im Verhältnis zum betroffenen Vertragsstaat sicherzustellen, dass keine Beeinträchtigung ausländischer Souveränität vorliegt. Beim grenzüberschreitenden Datenzugriff haben sie jedoch weiterhin die inländischen prozessualen Regeln einzuhalten. Demzufolge vermag Art. 32 CCC keine originären Zwangsmassnahmen zu begründen, sondern erlaubt Verfahrenshandlungen im Ausland, soweit diese auch im inländischen Prozessrecht zulässig sind.[132]

Art. 32 lit. a CCC kann OSINT nur so weit legitimieren, wie das innerstaatliche Recht den Zugang und die Auswertung öffentlich zugänglicher Daten durch Strafverfolgungsbehörden nicht einschränkt.[133] Die Massnahmen müssen folglich auch im innerstaatlichen Strafprozessrecht rechtmässig sein. Das kann bei minimalinvasiven Sachverhalten bejaht werden. Für Massnahmen, welche die Reichweite der Einwilligung übersteigen sowie für schwerwiegende OSINT-Massnahmen müssten im innerstaatlichen Recht gesetzliche Grundlagen bestehen.

3. Innerstaatliche Bestimmungen

Das Heranziehen der strafprozessualen Gesamtordnung als „Generalklausel" kann nur für minimalinvasive OSINT-Verfahren überzeugen, die aufgrund der Einwilligung den grundrechtlichen Schutzbereich nur noch hinsichtlich seines programmatischen Charakters berühren. Für alle anderen Verfahren wäre eine Gesetzesnorm heranzuziehen. Infrage kommen im innerstaatlichen Recht die Bestimmungen zur Durchsuchung von Aufzeichnungen (Art. 246 ff. StPO), zur Observation (Art. 282 f. StPO) sowie zur allgemeinen Datenbearbeitung (Art. 95 ff. StPO).

Mit OSINT werden Informationen erhoben, die auf Servern der jeweiligen Online-Dienste gespeichert werden. Server sind eine besondere Form physischer Datenträger, die elektronische Informationen enthalten. Sie unterliegen

---

131 DOMBROWSKI, 158; zu den Ausführungen im Explanatory Report CCC, Rz. 293.

132 Onlinekommentar CCC-GRAF, Art. 32 Rz. 17; vgl. ebenfalls WALDER, 542, jedoch in Bezug auf Art. 32 lit. b CCC.

133 So die Auslegung des Cybercrime Convention Committee von Art. 32 lit. a CCC, siehe Guidance #3, Transborder access to data (Article 32), 4 Fn. 3, abrufbar unter <https://rm.coe.int/16802e726a>.

grundsätzlich der Durchsuchung von Aufzeichnungen i.S.v. Art. 246 StPO, welche die Durchsuchung von Datenträgern erlaubt. Sie erstreckt sich jedoch nur auf die körperlichen Gegenstände, auf oder in denen die Informationen aufgezeichnet sind.[134] Open Source-Ermittlungen sind nicht darauf ausgerichtet, physisch verfügbare Datenträger zu durchsuchen, sondern Inhalte im Internet. Aufgrund seiner Beschaffenheit als Netzwerk stellt das Internet kein taugliches Durchsuchungsobjekt i.S.v. Art. 246 StPO dar. OSINT lässt sich deshalb nicht auf Art. 246 ff. StPO stützen.[135] Dass sich der Inhaber der Aufzeichnungen gemäss Art. 247 f. StPO vorgängig zum Inhalt der Aufzeichnungen äussern und die Siegelung beantragen kann, verdeutlich diese Einordnung. Dies wäre bei OSINT geradezu unmöglich.

Da OSINT mitunter als Beobachtung von Online-Aktivitäten verstanden werden kann, hat das Vorgehen Ähnlichkeit mit einer Observation i.S.v. Art. 282 StPO. Bei einer Observation werden Personen und Sachen an allgemein zugänglichen Orten verdeckt während einer gewissen Dauer beobachtet.[136] Unter allgemein zugänglichen Orten wurden bislang physisch zugängliche Räume wie Strassen, Bahnhöfe oder Parkanlagen gefasst.[137] Auch der öffentliche Teil des Internets kann als allgemein zugänglich verstanden werden, weshalb Observationen im virtuellen Raum denkbar sind. Eine solche Online-Observation kann angenommen werden, wenn das Verhalten von Zielpersonen im Internet laufend, d.h. in Echtzeit beobachtet wird. Dies wäre bspw. bei der Live-Beobachtung des Online-Verhaltens einer Person in einem Webforum der Fall. Nicht auf Art. 282 StPO stützen lassen sich jedoch OSINT-Methoden, mit denen bestehende Inhalte im Netz mittels Web Crawling oder Web Scraping bearbeitet werden, da dies keine virtuelle Beobachtung in Echtzeit darstellt und nicht der Natur der Observation entspricht. Gezieltes Monitoring des aktuellen Online-Verhaltens einer Zielperson findet in Art. 282 StPO jedoch eine Gesetzesgrundlage.

Mit Art. 95 ff. StPO bestehen schliesslich allgemeine Regeln für Datenbearbeitungen durch Strafverfolgungsbehörden. Die Bestimmungen halten allgemeine Grundsätze fest wie bspw. derjenige der Transparenz bei der Beschaf-

---

134 SK StPO-Keller, Art. 246 Rz. 6; vgl. BSK StPO 2023-Thormann/Brechbühl, Art. 246 Rz. 3; PK StPO-Jositsch/Schmid, Art. 246 Rz. 2.

135 Im Ergebnis ebenso Cartner/Schweingruber, 996.

136 Botschaft des Bundesrates vom 21. Dezember 2005 zur Vereinheitlichung des Strafprozessrechts, BBl 2005 1085 ff., 1252.

137 Siehe bspw. die Aufzählung von physischen Orten in: PK StPO-Jositsch/Schmid, Art. 282 Rz. 7.

fung von Daten (Art. 95 StPO). Mit diesen Normen sollten gewisse Prinzipien des Datenschutzrechts in die StPO übernommen werden, da hängige Strafverfahren vom Anwendungsbereich des DSG ausgeschlossen sind (Art. 2 Abs. 3 DSG).[138] Ein Teil der Lehre sieht in Art. 95 StPO eine gesetzliche Grundlage für Datenbeschaffungen.[139] Cartner und Schweingruber[140] sowie Graf[141] erachten deshalb Art. 95 StPO auch als taugliche gesetzliche Grundlage für Open-Source-Ermittlungen. Bei genauer Betrachtung normiert Art. 95 StPO jedoch bloss den Grundsatz und die Pflicht transparenter Datenbeschaffung, äussert sich aber nicht dazu, zu welchen Zwecken und unter welchen Voraussetzungen Daten beschafft werden dürfen. Auch die gesetzessystematische Einordnung der Norm im 8. Kapitel bei den allgemeinen Verfahrensregeln weist darauf hin, dass die Bestimmungen allein keine Grundrechtseingriffe zu Beweiserhebungszwecken rechtfertigen. Sie sind deshalb auch nicht im 5. Titel der StPO im Katalog der Zwangsmassnahmen zu finden. Wenn überhaupt können die Art. 95 ff. StPO ergänzend herangezogen werden, um OSINT an die datenschutzrechtlichen Prinzipien zu binden.

VI. Fazit

Öffentlich zugängliche Informationen bergen enormes kriminalistisches Potenzial. So vielfältig die Informationen sind, so divers sind auch die Methoden, an diese zu gelangen. OSINT-Anwendungen im Strafverfahren reichen vom Googeln einzelner Personen über die automatisierte Textinhaltsanalyse von Tweets bis hin zur biometrischen Auswertung von Gesichtsbildern. Mit der Bandbreite an Open Source-Kategorien variiert auch deren rechtliche Bewertung.

Werden mit Open Source-Ermittlungen Personendaten beschafft (und/oder bekanntgegeben), stellt dies eine staatliche Datenbearbeitung dar, die in den Schutzbereich von Art. 13 Abs. 2 BV fällt. Die eigenständige Veröffentlichung der Daten durch betroffene Personen kann in gewissen Fällen als (mutmassliche) Einwilligung in die Einsichtnahme interpretiert werden. Damit wird der Eingriff geradezu minimalinvasiv. Da Grundrechte nicht nur individualrechtlichen, sondern auch programmatischen Charakter haben, entfallen die sich

138 BBl 2005 1159; vgl. BSK StPO 2023-Fiolka, Vor Art. 95 ff. Rz. 2.

139 BSK StPO 2023-Fiolka, Art. 95 N 1; implizit ebenso SK StPO-Brüschweiler/Grüning, Art. 95 Rz. 1.

140 Cartner/Schweingruber, 994.

141 Onlinekommentar CCC-Graf, Art. 32 Rz. 17.

aus dem Legalitätsprinzip ergebenden Ansprüche an gesetzliche Grundlagen trotzdem nicht vollends. Wie die Abhandlung aufzeigte, gibt es zudem zahlreiche OSINT-Kategorien, bei denen nicht ohne Weiteres auf das Vorliegen einer Einwilligung geschlossen werden kann oder die gar schwere Grundrechtseingriffe darstellen.

Vorliegen und Reichweite der Einwilligung sowie Schwere des Eingriffs sind deshalb für jede Methode gesondert zu beurteilen. Bei minimalinvasiven Recherchen, für die eine Einwilligung anzunehmen ist, kann die gesetzliche Grundlage in den allgemeinen rechtlichen Leitplanken der StPO erblickt werden. Leichte Massnahmen, welche eine (mutmassliche) Einwilligung übersteigen sowie schwere Massnahmen bedürften jedoch spezialgesetzlicher Grundlagen.

De lege lata enthält die StPO keine OSINT-Bestimmungen. Die Art. 246 ff. StPO erlauben die Durchsuchung einzelner Gegenstände, nicht aber des gesamten Internets. Die Bestimmungen der Observation (Art. 282 f. StPO) lassen sich in spezifischen Konstellationen der länger andauernden Beobachtung, d.h. eines eigentlichen Online-Monitorings einer Zielperson, heranziehen. Die konventionsrechtliche Grundlage in Art. 32 lit. a CCC rechtfertigt schliesslich Massnahmen nur insoweit, als diese auch im innerstaatlichen Verhältnis rechtmässig sind. Dies ist momentan nur bei minimalinvasiven Eingriffen sowie beim eben genannten Echtzeit-Monitoring der Fall. Für invasivere Massnahmen wie Web Scraping oder intelligente Datenweiterbearbeitungen bestehen im geltenden Recht keine Grundlagen.

Es zeigt sich einmal mehr, dass die StPO nicht auf neue digitale Ermittlungsmassnahmen vorbereitet ist. Auch wenn mit digitalen Ermittlungsmethoden kein physischer Zwang einhergehen mag, handelt es sich bei Datenbearbeitungen zum Zwecke der Strafverfolgung um Zwangsmassnahmen, die hinreichend bestimmte gesetzliche Grundlagen bedürfen. In Anbetracht der Praxisrelevanz von OSINT wäre es angezeigt, sie explizit zu normieren. Damit würden erkennbare Grenzen gesetzt, welche Formen von Open Source-Ermittlungen zum Einsatz kommen sollen – und welche nicht.

Literaturverzeichnis

Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz (DSG), Stämpflis Handkommentar, 2. A., Bern 2023 (zit.: SHK DSG-Bearbeiter/in, Art. XX Rz. YY).

Barthe Christoph/Gericke Jan (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung, 9. A., München 2023 (zit.: KK StPO-Bearbeiter/in, § XX Rz. YY).

Bauer Sebastian, Soziale Netzwerke und strafprozessuale Ermittlungen, Diss. Berlin 2018.

Becker Maximilian/Becker Felix, Die neue Google-Datenschutzerklärung und das Nutzer-Metaprofil, MMR 2012, 351 ff.

Biaggini Giovanni (Hrsg.), Kommentar zur Schweizerischen Bundesverfassung, 2. A., Zürich 2017 (zit.: OFK BV-Bearbeiter/in, Art. XX Rz. YY).

Bieresborn Dirk, Unzulässige Drittstaatenübermittlung durch „Googlen"? Zeitschrift für Datenschutz, ZD 2016, 319 ff.

Bieri Adrian/Powell Julian (Hrsg.), DSG, Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zürich 2023 (zit.: OFK DSG-Bearbeiter/in, Art. XX. Rz. YY).

Büchi Moritz/Festic Noemi/Latzer Michael, The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical Research Agenda, Big Data & Society 2022, abrufbar unter <https://journals.sagepub.com/doi/10.1177/20539517211065368>.

Cartner Anna/Schweingruber Sandra, Strafbehörden dürfen googlen, AJP 2021, 990 ff.

Dombrowski Nadine, Extraterritoriale Strafrechtsanwendung im Internet, Berlin 2014.

Donatsch Andreas/Lieber Viktor/Summers Sarah/Wohlers Wolfang (Hrsg.), Kommentar zur Schweizerischen Strafprozessordnung, Schulthess Kommentar, 3. A., Zürich 2020 (zit. SK StPO-Bearbeiter/in, Art. XX Rz. YY).

Ehrenzeller Bernhard et al. (Hrsg.), Die schweizerische Bundesverfassung, St. Galler Kommentar, 3. A., Zürich/St. Gallen 2023 (zit.: SGK BV-Bearbeiter/in, Art. XX Rz. YY).

Eicker Andreas/Mango-Meier Sonja, Bundesgericht, Strafrechtliche Abteilung, Urteil 6B_996/2016 vom 11. April 2017, X., A. GmbH, B. gegen Staatsanwaltschaft des Kantons St. Gallen, Anordnungskompetenz der Polizei und Wirkung der Einwilligung der betroffenen Person, Entschädigung und Genugtuung (Einstellung), AJP 2018, 660 ff.

Fasnacht Tobias, Die Einwilligung im Datenschutzrecht, Diss. Fribourg, Zürich 2017.

Flückiger Alexandre, L'autodétermination en matière de données personnelles: un droit (plus si) fondamental à l'ère digitale ou un nouveau droit depropriété? AJP 2013, 837 ff.

Gächter Thomas/Werder Gregori, Einbettung ausgewählter Konzepte in das schweizerische Datenschutzrecht, Forum Europarecht 2013, 87 ff.

Gibson Helen, Acquisition and Preparation of Data for OSINT Investigations, in: Akhgar Babak/Bayerl Saskia P./Sampson Fraser (Hrsg.), Open Source Intelligence Investigation, Cham 2016, 78 ff.

Glass Philippe, Die rechtsstaatliche Bearbeitung von Personendaten in der Schweiz, Diss. Basel, Zürich 2016.

Graf Damian K. (Hrsg.), Onlinekommentar Übereinkommen über die Cyberkriminalität (Cybercrime Convention) – Version 26.10.2023, abrufbar unter <https://onlinekommentar.ch/de/kommentare/ccc32> (zit. Onlinekommentar CCC-Bearbeiter/in, Art. XX Rz. YY).

Graf Damian K., Strafverfolgung 2.0: Direkter Zugriff der Strafbehörden auf im Ausland gespeicherte Daten? Jusletter IT, 21. September 2017 (zit. Strafverfolgung 2.0).

Graf Jürgen (Hrsg.), Beck'scher Onlinekommentar StPO mit RiStBV und MiStra, 49. Lieferung, München 2023 (zit.: BeckOK StPO-Bearbeiter/in, § XX Rz. YY).

Häner Isabelle, Die Einwilligung der betroffenen Person als Surrogat der gesetzlichen Grundlage bei individuell-konkreten Staatshandlungen, ZBl 2002, 57 ff.

Hansjakob Thomas, Verdeckte polizeiliche Tätigkeit im Internet, forumpoenale 2014, 244 ff.

Harasgama Rehana, Erfahren – Wissen – Vergessen, Zur zeitlichen Dimension des staatlichen Informationsanspruches, Diss. St. Gallen, Zürich 2017.

Harwell Drew, This Facial Recognition Website Can Turn Anyone into a Cop-or a Stalker, in: Martin Kristen (Hrsg.), Ethics of Data and Analytics, New York 2022, 63 ff.

Heydon Allan/Najork Marc, Mercator: A scalable, extensive Web crawler, World Wide Web 1999, 219 ff.

Joint Statement on data scraping and the protection of privacy, 24. August 2023, abrufbar unter <https://ico.org.uk/media/about-the-ico/documents/4026232/joint-statement-data-scraping-202308.pdf>.

Jositsch Daniel/Schmid Niklaus, Schweizerische Strafprozessordnung, Praxiskommentar, 4. A., Zürich/St. Gallen 2023 (zit.: PK StPO-Jositsch/Schmid, Art. XX Rz. YY).

Kausar Abu Md./Dhaka V.S./Kumar Singh Snajeev, Web Crawler: A Review, International Journal of Computer Applications 2013, 31 ff.

Kiener Regina/Kälin Walter/Wyttenbach Judith, Grundrechte, 3. A., Bern 2018.

Knauer Christoph/Kudlich Hans/Schneider Hartmut (Hrsg.), Münchener Kommentar zur StPO, Band 2, München 2016 (zit.: MüKO StPO-Bearbeiter/in, § XX Rz. YY)

Köver Chris, Netzpolitik vom 21. November 2022, „PimEyes droht eine Millionenstrafe", abrufbar unter <https://netzpolitik.org/2022/bussgeldverfahren-aus-dem-laendle-pimeyes-droht-eine-millionenstrafe/>.

Krause Benjamin, Ermittlungen im Darknet – Mythos und Realität, Neue Juristische Wochenschrift, NJW 2018, 657 ff.

Krotov Vlad/Silva Leiser, Legality and Ethics of Web Scraping, American Conference on Information Systems 2018, 1 ff.

Logos Katie et al., Establishing a framework for the ethical and legal use of web scrapers by cybercrime and cybersecurity researchers: learnings from a systematic review of Australian research, International Journal of Law and Information Technology 2023, abrufbar unter <https://academic.oup.com/ijlit/article/31/3/186/7289618>.

Luccioni Alexandra/Viviano Joseph, What's in the Box? A Preliminary Analysis of Undesirable Content in the Common Crawl Corpus, Proceedings of the 59th Annual Meeting of the Association for Computational Linguistics 2021, 182 ff.

Ludewig Franziska/Epple Günther, Open Source Intelligence zur Einsatzbewältigung in der Polizei, Kriminalistik 2020, 457 ff.

Maeder Stefan/Stadler Marcus, Strafprozessuale Videoüberwachung und informationelle Selbstbestimmung – Anmerkungen zu BGE 145 IV 32, forumpoenale 2019, 396 ff.

Malacrida Ralph, Der Grundrechtsverzicht, Diss. Zürich 1992.

Mohn Matthias, Dürfen Arbeitnehmer ChatGPT zur Erledigung ihrer Aufgaben einsetzen? Neue Zeitschrift für Arbeitsrecht, NZA 2023, 538 ff.

Montero Sabrina/Simon Manon Céline, Die Rechtmässigkeit der „freiwilligen“ Hausdurchsuchung ohne Durchsuchungsbefehl, forumpoenale 2017, 99 ff.

Müller Jörg Paul/Schefer Markus, Grundrechte in der Schweiz, 4. A., Bern 2008.

Müller Lucien, Videoüberwachung in öffentlich zugänglichen Räumen – insbesondere zur Verhütung und Ahndung von Straftaten, Diss. St. Gallen, Zürich 2011.

Niggli Marcel Alexander/Heer Marianne/Wiprächtiger Hans (Hrsg.), Schweizerische Strafprozessordnung (StPO), Basler Kommentar, 1. A., Basel 2010 (zit.: BSK StPO 2010-Bearbeiter/in, Art. XX Rz. YY).

Niggli Marcel Alexander/Heer Marianne/Wiprächtiger Hans (Hrsg.), Schweizerische Strafprozessordnung (StPO), Basler Kommentar, 2. A., Basel 2017 (zit.: BSK StPO 2017-Bearbeiter/in, Art. XX Rz. YY).

Niggli Marcel Alexander/Heer Marianne/Wiprächtiger Hans (Hrsg.), Schweizerische Strafprozessordnung (StPO), Basler Kommentar, 3. A., Basel 2023 (zit.: BSK StPO 2023-Bearbeiter/in, Art. XX Rz. YY).

Oberholzer Niklaus, Grundzüge des Strafprozessrechts, 4. A., Bern 2020.

Rezende Isadora Neroni, Facial recognition in police hands: Assessing the ‘Clearview case’ from a European perspective, New Journal of European Criminal Law 2020, 375 ff.

Rückert Christian, Mit künstlicher Intelligenz auf Verbrecherjagd, 22. Januar 2021, abrufbar unter <https://verfassungsblog.de/ki-verbrecherjagd/> (zit. Rückert, Verbrecherjagd).

Rückert Christian, Zwischen Online-Streife und Online-(Raster-)Fahndung – Ein Beitrag zur Verarbeitung öffentlich zugänglicher Daten im Ermittlungsverfahren, Zeitschrift für die gesamte Strafrechtswissenschaft, ZStW 2017, 302 ff. (zit. Rückert, Online-Streife)

Rückert Christian, Digitale Daten als Beweismittel im Strafverfahren, Habil. Friedrich-Alexander-Universität Erlangen-Nürnberg 2022, Tübingen 2023 (zit. Rückert, Digitale Daten).

Schwartz Candy, Web Search Engines, Journal of the American Society for Information Science 1998, 973 ff.

Seymour Tom/Frantsvog Dean/Kumar Satheesh, History of Search Engines, International Journal of Management & Information Systems 2011, 47 ff.

Sieber Ulrich/Brodowski Dominik, Teil 19.3 Strafprozessrecht, in: Hoeren Thomas/Sieber Ulrich/Holznagel Bernd (Hrsg.), Handbuch Multimedia-Recht, 59. Lieferung, München 2023.

Van Spyk Benedikt, Das Recht auf Selbstbestimmung in der Humanforschung, Diss. St. Gallen, Zürich 2011.

Voigt Paul, Datenschutz bei Google, Multimedia und Recht, Zeitschrift für IT-Recht und Recht der Digitalisierung, MMR 2009, 377 ff.

Walder Stephan, Grenzüberschreitende Datenerhebung: Ist und Soll, Kriminalistik 2020, 540 ff.

Waldmann Bernhard/Belser Eva Maria/Epiney Astrid (Hrsg.), Schweizerische Bundesverfassung (BV), Basler Kommentar, Basel 2015 (zit.: BSK BV-Bearbeiter/in, Art. XX Rz. YY).

Wittmer Sandra/Platzer Florian, Zulässigkeit von Open Source-Ermittlungen zur Strafverfolgung im Darknet, Informatik 2022, 569 ff.

Woerlein Andreas H., ChatGPT – „Fortschritt“ durch Künstliche Intelligenz auf Kosten des Datenschutz- und Urheberrechts, Zeitschrift für Datenschutz, ZD-aktuell 2023, 01205.

Zhuoli Chen, Einwilligung als Ersatz des Durchsuchungsbefehls? – Am Beispiel der Hausdurchsuchung ohne Durchsuchungsbefehl, forumpoenale 2015, 298 ff.

Zimmerlin Sven, Der Verzicht des Beschuldigten auf Verfahrensrechte im Strafprozess: zugleich ein Betrag zum Grundrechtsverzicht, Diss. Zürich 2008.

RISIKO RECHT

2. Jahrgang

HERAUSGEBER

WISSENSCHAFTLICHER BEIRAT

REDAKTION

Dr. Tobias Baumgartner, LL.M., Rechtsanwalt /
MLaw Sophie Tschalèr
Europa Institut an der Universität Zürich
Hirschengraben 56
8001 Zürich
Schweiz

ERSCHEINUNGSWEISE

R&R – Risiko & Recht erscheint dreimal jährlich online. Die Ausgaben werden zeitgleich im Wege des print on demand veröffentlicht; sie können auf der Verlagswebseite (www.eizpublishing.ch) sowie im Buchhandel bestellt werden.

ZITIERWEISE

R&R, Ausgabe 1/2023, ...

KONTAKT

EIZ Publishing
c/o Europa Institut an der Universität Zürich
Dr. Tobias Baumgartner, LL.M., Rechtsanwalt
Hirschengraben 56
8001 Zürich
Schweiz
eiz@eiz.uzh.ch

ISSN

2813-7841 (Print)
2813-785X (Online)

ISBN:

978-3-03805-665-2 (Print – Softcover)
978-3-03805-666-9 (PDF)
978-3-03805-667-6 (ePub)

VERSION

1.03-20240319

DOI

Zeitschrift: https://doi.org/10.36862/eiz-rrz01
Ausgabe: https://doi.org/10.36862/eiz-rr202401
Alexandra Ott Müller / Sven Zimmerlin, Kinder und Jugendliche im Umfeld von Gewalt – Aufgaben und Möglichkeit der Jugendstrafrechtspflege, https://doi.org/10.36862/eiz-rr202401-01
Andrea Selle, Staatshaftung im Rahmen der Erfüllung sicherheitspolizeilicher Aufgaben durch Private, https://doi.org/10.36862/eiz-rr202401-02
Monika Simmler / Giulia Canova, Rechtmässigkeit von Open Source-Ermittlungen durch Strafverfolgungsbehörden, https://doi.org/10.36862/eiz-rr202401-03

RISIKO

EIZ Publishing

Herausgeber:
Prof. Dr. Tilmann Altwicker
PD Dr. Goran Seferovic
Prof. Dr. Franziska Sprecher
Prof. Dr. Stefan Vogel
Dr. Sven Zimmerlin

RISIKO & RECHT **AUSGABE 01 / 2024**

RECHT