RUHR-UNIVERSITÄT BOCHUM | 44780 Bochum | Germany

JURISTISCHE FAKULTÄT

Juniorprofessur für Kriminologie, Strafrecht und Sicherheitsforschung im digitalen Zeitalter
Universitätsstr. 150
44780 Bochum

JUN.-PROF. DR. SEBASTIAN GOLLA
sebastian.golla@rub.de
www.jura.rub.de/jpkrim

03. Juni 2024

Abschlussbericht

Verbundprojekt:
Einsatz von KI zur Früherkennung von Straftaten (KISTRA)

Teilvorhaben:
Rechtliche Rahmenbedingungen

Förderkennzeichen:
13N15339

Laufzeit des Vorhabens:
01.07.2020-31.12.2023

Berichtszeitraum:
01.07.2020-31.12.2023

Ansprechpartner:
Jun.-Prof. Dr. Sebastian Golla
Juniorprofessur für Kriminologie, Strafrecht und Sicherheitsforschung im digitalen Zeitalter
Ruhr-Universität Bochum
Juristische Fakultät
Universitätsstr. 150
44780 Bochum
sebastian.golla@rub.de

Inhaltsverzeichnis

A. Ziele

Das Teilvorhaben „Rechtliche Rahmenbedingungen“ hat zwei Arbeitsziele verfolgt. Das erste Arbeitsziel bestand darin, den Rechtsrahmen für den Einsatz von Methoden Künstlicher Intelligenz (KI) in den für den Verbund festgelegten Szenarien auszuleuchten, in der Folge einen Leitfaden für die rechtskonforme und datenschutzverträgliche Implementierung der technischen Lösungen zu erarbeiten und diesen schließlich umzusetzen. Das zweite Arbeitsziel besteht darin, die Möglichkeiten zu untersuchen, von Betreiber:innen sozialer Medien (im Folgenden: Telemediendienstanbieter:innen (TMDA) die Eröffnung von Datenzugängen zugunsten von Sicherheitsbehörden zu verlangen.

Für das erste Arbeitsziel waren auf verfassungsrechtlicher Ebene zunächst die Rahmenbedingungen für den Einsatz von Künstlicher Intelligenz zur Erkennung, Vorbeugung und Verfolgung von Straftaten zu betrachten. Dies erforderte eine Auseinandersetzung mit dem Grundrecht auf informationelle Selbstbestimmung bzw. dem Datenschutzgrundrecht und dem Diskriminierungsverbot aus Art. 3 Abs. 3 GG sowie weiteren Grundrechten. Von besonderer Bedeutung war dabei einerseits die Intensität des Grundrechtseingriffs, wenn ursprünglich manuelle Tätigkeiten, etwa die Auswertung von Daten, automatisiert durch den Einsatz der Software erfolgen. Daran schloss sich andererseits die erschwerte rechtliche Kontrolle der Software-Ergebnisse an, die ein Verständnis der technischen Funktionsweise sowie einen reflektierten Umgang mit den Resultaten notwendig machen. Insbesondere das Verbot automatisierter Einzelentscheidungen ohne eigenständige Rechtsgrundlage (§ 54 BDSG) war auch auf einfachgesetzlicher Ebene zu berücksichtigen. Daraus folgt, dass ein vollautomatisierter Einsatz ohne menschliche Intervention rechtlich unzulässig ist. Für die weiterführende Frage, ob die Software entscheidungsunterstützend eingesetzt werden kann, waren die jeweils einschlägigen Rechtsgrundlagen aus dem Polizei- oder Strafverfahrensrecht heranzuziehen.

Für das zweite Arbeitsziel wurden mögliche Mitwirkungspflichten der TMDA bei der Bekämpfung und Löschung strafbarer Hassrede untersucht. Hierbei war das Spannungsverhältnis zwischen den Rechten der Unternehmen und ihrer Nutzer:innen und dem sicherheitsbehörtlichen Interesse an der Datenübermittlung auf verfassungsrechtlicher und einfachgesetzlicher Ebene, unter Einbeziehung unionsrechtlicher Rechtsprechung, abzuwägen.

B. Arbeitsplan

Das Teilvorhaben „Rechtliche Rahmenbedingungen“ hat einen Beitrag zu Arbeitspaket 1 erbracht. Dieser unterteilt sich im die Teil-AP 1.1 – Bedarfsanalyse und Nutzeranforderungen (3 PM in M 1-3), 1.4 – Verfassungsrechtliche und eingriffsrechtliche Analyse (20 PM in M 4-36) sowie 1.5 – Erarbeitung von Leitlinien (4 PM – M 19-30). Der Meilenstein des Teilvorhabens bestand in einem Zwischenbericht zu den rechtlichen Rahmenbedingungen des Einsatzes von Methoden Künstlicher Intelligenz zu den definierten Zwecken. Dieser lag als Zwischenstand von AP 1.4 bis zum Ende des achtzehnten Projektmonats vor. Als Abbruchkriterium wurde vorab definiert, dass das Projekt abzubrechen wäre, wenn der Zwischenbericht zu dem Ergebnis käme, dass der Teildemonstrator schon den verfassungsrechtlichen Rahmenbedingungen nach nicht einsetzbar wäre.

Zu Beginn des Projektes wurde der Prozess der Bedarfsanalyse im Rahmen des AP 1.1 begleitet, um bereits frühzeitig auf etwaige rechtliche Probleme aufmerksam zu werden. Hierzu fanden verschiedene Austauschformate mit der Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW), dem Bundeskriminalamt (BKA) und der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) statt, die gemeinsam mit der TU Berlin und der RWTH Aachen ausgewertet wurden. Im Anschluss an die Auswertung der Gespräche wurde für die weitere wissenschaftliche Untersuchung zwischen ZMI-Prozess und ST-Prozess differenziert. Ersterer beschreibt das Vorgehen der Zentralen Meldestelle für strafbare Inhalte im Internet beim BKA (ZMI), an die Hinweise auf strafbare Hassrede übermittelt werden. Letzterer bezeichnet das Vorgehen des polizeilichen Staatsschutzes beim BKA (ST), der proaktive Auswertungen hinsichtlich strafbarer Inhalte tätigt oder im Rahmen größerer Ermittlungskomplexe Zugang zu entsprechenden Daten erhält. Aus dem ZMI- sowie ST-Prozess wurden fünf Szenarien gebildet, die der eingriffsrechtlichen Untersuchung zu Grunde gelegt wurden.

Das dem Forschungsprozess zu Grunde liegende Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität enthielt in seiner zunächst am 18.06.2020 im Bundestag und am 03.07.2020 im Bundesrat beschlossenen Fassung Regelungen zur Bestandsdatenauskunft, die erkennbar gegen die jüngsten Vorgaben des

Bundesverfassungsgerichts[1] verstießen. Daraufhin wurde das Gesetz zunächst nicht vom Bundespräsidenten ausgefertigt und noch einmal im parlamentarischen Verfahren überarbeitet. In seiner endgültigen Fassung ist das Gesetz schließlich erst am 26.03.2021 beschlossen und am 02.04.2021 im Bundesgesetzblatt verkündet worden. Nach Verkündung des Gesetzes traten die neuen Regelungen überwiegend zum 01.07.2021 in Kraft. Eine Ausnahme bildeten die Änderungen im Netzwerkdurchsetzungsgesetz (NetzDG), die erst zum 01.02.2022 in Kraft traten und TMDA verpflichten, das Verbreiten bestimmter strafbarer Inhalte an das Bundeskriminalamt zu melden.

Die in AP 1.4 vorgesehene verfassungsrechtliche und eingriffsrechtliche Analyse setzt die Kenntnis der rechtlichen Grundlage voraus, auf deren Basis die Meldung strafbarer Inhalte durch die TMDA und der KI-Einsatz im BKA bei der Bewertung dieser Inhalte erfolgen kann. An dieser Rechtsgrundlage fehlte es in den ersten neun Monaten des Projektes. Insbesondere wurde die Regelung zur sog. Bestandsdatenauskunft im parlamentarischen Verfahren noch einmal grundlegend neugestaltet. Diese Regelung ist für den Geschäftsprozess im BKA jedoch zentral, weil anhand der Bestandsdatenauskunft die Zuständigkeit der anschließend tätig werdenden Strafverfolgungs- oder Gefahrenabwehrbehörde bestimmt wird. Um diesen Nachteil auszugleichen, wurde der Gesetzgebungsprozess detailliert begleitet und dazu abgegebene Stellungnahmen von Sachverständigen sowie die wissenschaftliche Kommentierung des Vorhabens ausgewertet. Zudem wurden erste Recherchen zur geltenden Rechtslage bzgl. der Möglichkeit des KI-Einsatzes im polizeilichen Eingriffsrecht getätigt, die zwar unabhängig von der gesetzlichen Neuregelung erfolgten, aber auf diese übertragbar sind. Insofern konnten die Verzögerung im Gesetzgebungsverfahren im Laufe des Forschungsprojektes aufgeholt werden.

Schließlich wurde in AP 1.5 Leitlinien für die rechtskonforme und datenschutzverträgliche Implementierung der technischen Lösungen erarbeitet. Vorläufige Erkenntnisse zu diesen Leitlinien – etwa die Bedeutung der Erklärbarkeit von Software-Ergebnissen – wurden im Projektverlauf immer wieder zwischen den beteiligten Forschungsinstitutionen thematisiert, damit sie bereits in die Entwicklung einbezogen werden können. Die abschließende Version

[1] Vgl. Bundesverfassungsgericht, Beschluss vom 27.05.2020, 1 BvR 1873/13, 1 BvR 2618/13.

der Leitlinien wurde schließlich beim Verbundtreffen am 30.11./01.12.2023 vorgestellt und diskutiert.

C. Ergebnisse

Die im Projekt entwickelte Software wirft diverse rechtliche Fragen auf. Im Ausgangspunkt wurde untersucht, in welche Grundrechte der staatliche Einsatz der Software eingreifen würde und an welchen Maßstäben dieser Eingriff zu prüfen ist (I.). Anschließend wurden allgemeine datenschutzrechtliche Anforderungen formuliert (II.) und die spezifischen eingriffsrechtlichen Anforderungen dargelegt (III.). Dabei wurden sowohl gefahrenabwehrrechtliche als auch strafprozessuale Aspekte berücksichtigt. Aufbauend auf die eingriffsrechtliche Analyse wurden Handlungsempfehlungen für die Implementation der Software formuliert (IV.). Schließlich wurden Erwägungen zu den infrastrukturellen Verpflichtungen der Betreiber:innen sozialer Netzwerke angestellt (V).

I. Verfassungsrecht

Zu Beginn der Entwicklung rechtlicher Maßstäbe für die Bewertung der geschilderten Szenarien stellt sich aus verfassungsrechtlicher Perspektive die Frage, inwiefern der staatliche Einsatz der Software einen Eingriff in die Grundrechte der betroffenen Personen bedeuten würde und nach welchen Kriterien sich ggf. die Intensität solcher Eingriffe bestimmen lässt. Grundsätzlich erfordert jeder Grundrechtseingriff eine Rechtsgrundlage. Grundrechte sind zunächst Abwehrrechte gegenüber dem Staat, begrenzen also die Möglichkeit staatlicher Eingriffe in die verfassungsrechtlich geschützten Freiheiten der Bürger:innen. Zugleich handelt es sich bei Grundrechten um objektive Wertentscheidungen, die bei jedem staatlichen Handeln zu achten und zu schützen sind. Im Zuge technischer Entwicklungen müssen staatliche Grundrechtseingriffe verhältnismäßig ausgestaltet sein.

1. Grundrecht auf informationelle Selbstbestimmung

Den wesentlichen Maßstab für die verfassungsrechtliche Bewertung des Demonstrators setzt das Recht auf informationelle Selbstbestimmung. Dieses aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG hergeleitete Recht hat sein Fundament in der Menschenwürde. Dem „Datenschutzgrundrecht“ liegt unter anderem der Gedanke zu Grunde, dass die „freie

Entfaltung der Persönlichkeit […] unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus[setzt]. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."[2]

a. Schutzbereich

Dieser weite Schutzumfang des informationellen Selbstbestimmungsrechts ist der abstrakten Gefährdungslage moderner Datenverarbeitungstechniken geschuldet. Diese Gefährdungslage kann „bereits im Vorfeld konkreter Bedrohungen benennbarer Rechtsgüter entstehen, insbesondere wenn personenbezogene Informationen in einer Art und Weise genutzt und verknüpft werden können, die der Betroffene weder überschauen noch verhindern kann."[3] Der Schutz knüpft unmittelbar an den Umgang mit jeder Art von personenbezogenen Daten an. Zur Bestimmung des Begriffes „personenbezogene Daten" kann hierbei auf die gesetzliche Definition zurückgegriffen werden. Nach Art. 4 Nr. 1 DSGVO sind personenbezogene Daten „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person […] beziehen". Hinsichtlich der betreffenden Daten ist es unerheblich, welcher Aussagegehalt ihnen zukommt, solange ein Personenbezug vorhanden ist. Maßgeblich für den Schutzumfang ist der Personenbezug, nicht die „Privatheit" der jeweiligen Information.

Im Arbeitsprozess der ZMI werden von den TMDA für strafbar befundene Inhalte, der verwendete Username und die IP-Adresse mit Portnummer an das BKA übermittelt. Nach der Rechtsprechung des Bundesgerichtshofes und des Europäischen Gerichtshofes handelt es sich bei (dynamischen) IP-Adressen um personenbezogene Daten, wenn die Bestimmung der Person für die verarbeitende Stelle technisch und rechtlich möglich ist sowie keinen zum Nutzen der Information außer Verhältnis stehenden Aufwand darstellt.[4] Durch die Verknüpfung der Inhalte

[2] BVerfGE 65, 1 (43).
[3] BVerfGE 120, 274 (312).
[4] BGH, Urteil vom 16.05.2017, Az.: VI ZR 135/13; EuGH, Urteil vom 19.10.2016, Az.: C-582/14.

mit dem Usernamen bzw. Account des:der Urheber:in besteht auch für die übermittelten Inhalte ein Personenbezug.

Im Arbeitsprozess bei ST lässt sich zurzeit noch nicht genau abschätzen, zur Bewertung welcher Inhalte die Software eingesetzt wird. Jedenfalls bei Daten, die im Rahmen einer polizeilichen Maßnahme, die sich gezielt gegen eine konkrete Person richtet, erhoben wurden, ist ein Personenbezug anzunehmen. Auch wird es sich bei einer Vielzahl von aus öffentlichen Quellen erhobenen Datensätzen um personenbezogene Daten handeln, da die Inhalte ihren Urheber:innen, etwa in sozialen Netzwerken, zuzuordnen sind. Ob die Personen dabei unter Klarnamen oder Pseudonymen agieren, spielt keine Rolle, solange die Möglichkeit besteht, sie mit einem zumutbaren Aufwand persönlich zu identifizieren. Die Daten von solchen Profilen in sozialen Netzwerken, die keine natürlichen Personen repräsentieren (z.B. Seiten oder Gruppen bei Facebook), fallen ebenfalls regelmäßig in den Schutzbereich. Zum einen stehen auch hinter diesen regelmäßig – z.B. über die Impressumsangabe – identifizierbare natürliche Personen und zum anderen können auch die Daten von juristischen Personen dem Schutzbereich unterfallen. Der Schutzbereich des informationellen Selbstbestimmungsrechts wird also aufgrund der Verarbeitung personenbezogener Daten in den beschriebenen Anwendungsszenarien oftmals eröffnet sein.

b. Eingriff

Grundsätzlich begründet jede Form des Umgangs mit personenbezogenen Daten einen Eingriff in das informationelle Selbstbestimmungsrecht. Darunter fallen neben der Erhebung und Speicherung der Daten unter anderem ihre Veränderung, Auswertung und Übermittlung. Dabei stellt jede Phase der Verarbeitung einen eigenständigen Eingriff dar, der für sich genommen rechtfertigungsbedürftig ist. Kein Grundrechtseingriff liegt hingegen grundsätzlich vor, wenn staatliche Stellen im Internet verfügbare Kommunikationsinhalte erheben, die allgemein zugänglich sind bzw. sich an einen nicht weiter abgrenzbaren Personenkreis richten. Dies gilt auch, wenn personenbezogene Daten erfasst werden. Ein Grundrechtseingriff kann allerdings gegeben sein, „wenn Informationen, die durch die Sichtung allgemein zugänglicher Inhalte gewonnen wurden, gezielt zusammengetragen, gespeichert und gegebenenfalls unter

Hinzuziehung weiterer Daten ausgewertet werden und sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt."[5]

Nach bisherigem Kenntnisstand werden im Arbeitsprozess der ZMI verschiedene personenbezogene Daten von den TMDA an das BKA übermittelt, durch die Software einer juristischen Prüfung unterzogen und anschließend von den zuständigen Sachbearbeiter:innen bewertet. Dann wird in der Regel zur Einleitung weiterer Strafverfolgungs- oder Gefahrenabwehrmaßnahmen eine Bestandsdatenauskunft zur Identifizierung der Nutzer:innen durchgeführt, die die übermittelten Inhalte veröffentlicht haben. Mit der Entgegennahme der von den TMDA übermittelten Informationen werden personenbezogene Daten beim BKA gespeichert. Mithin liegt ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung vor. Die straf- und gefahrenabwehrrechtlichen Bewertung der Daten durch den Einsatz der Software stellt zudem einen Datenverarbeitungsvorgang dar, der einen weiteren Eingriff in das Grundrecht bewirkt.

Im Arbeitsprozess von ST werden personenbezogene Daten, die im Rahmen polizeilicher Maßnahmen erhoben oder durch Private an das BKA übermittelt wurden, unter Einsatz der Software auf ihre strafrechtliche Relevanz hin ausgewertet. Bereits in der Erhebung dieser Daten wird regelmäßig ein Grundrechtseingriff liegen. Zudem soll die Internetauswertung durch den Einsatz von Methoden Künstlicher Intelligenz erweitert werden. Auch wenn diese Internetauswertung im Wesentlichen anhand von in sozialen Netzwerken ohne weitere Beschränkung veröffentlichten Inhalten erfolgt, ist die oben geschilderte Ausnahme, nach der bei der Sichtung allgemein zugänglicher Daten kein Grundrechtseingriff vorliegt, nicht einschlägig. Es handelt sich bei der polizeilichen Internetauswertung nämlich gerade um ein gezieltes Zusammentragen, Speichern und Auswerten, das eine besondere Gefahrenlage für die auf informationelle Selbstbestimmung der Betroffenen herbeiführt.

Vor allem hinsichtlich der Erweiterung der polizeilichen Internetauswertung durch Methoden Künstlicher Intelligenz stellt sich die Frage nach der Intensität der damit verbundenen Grundrechtseingriffe. Die Feststellung der Intensität ist wichtig, um die Anforderungen an die

[5] BVerfGE 120, 274 (345).

Rechtfertigung der Eingriffe zu bestimmen. In der Rechtsprechung haben sich dafür verschiedene Kriterien herausgebildet. Maßgeblich sind insbesondere die Streubreite der Maßnahme und die Persönlichkeitsrelevanz der betroffenen Daten. Besonders intensive Grundrechtseingriffe erhöhen damit die Anforderungen an die jeweilige Rechtsgrundlage, um gerechtfertigt werden zu können.

c. Rechtfertigung

Das Recht auf informationelle Selbstbestimmung ist jedoch nicht schrankenlos gewährleistet. Personenbezogene Daten ‚gehören' nicht der jeweiligen Person, sondern sind Abbild einer sozialen Realität innerhalb einer größeren Gemeinschaft. In den weit gefassten Schutzbereich des Grundrechts auf informationelle Selbstbestimmung kann deshalb durch oder aufgrund eines Gesetzes eingegriffen werden. Die Verarbeitung personenbezogener Daten kann daher gerechtfertigt sein, wenn sie auf einer gesetzlichen Grundlage erfolgt und verhältnismäßig ist.

Ob die bestehenden Rechtsgrundlagen die aus den jeweiligen Anwendungsszenarien hervorgehenden Eingriffe in das Recht auf informationelle Selbstbestimmung rechtfertigen können, wird im Gutachten zu AP 1.4 im Einzelnen dargelegt. Zur Wahrung des Grundsatzes der Verhältnismäßigkeit verlangt die Rechtsprechung für den Einsatz komplexer Datenverarbeitungsprozesse zudem Verfahrenssicherungen zur Herstellung von Transparenz, Rechtsschutz und Kontrolle. Die Transparenz der Datenverarbeitung soll den demokratischen Diskurs über den staatlichen Umgang mit Daten ermöglichen. Zugleich ist sie Voraussetzung für einen wirksamen Rechtsschutz der Betroffenen, damit diese die Rechtmäßigkeit der Maßnahmen gerichtlich überprüfen und subjektivrechtliche Ansprüche auf Löschung, Berichtigung oder Genugtuung geltend machen können. Ergänzt wird dies durch eine aufsichtsbehördliche Kontrolle der Datenverarbeitung. Deren Bedeutung ist umso größer, wenn es sich bei der Datenverarbeitung um einen Grundrechtseingriff handelt, der für die Betroffenen nicht unmittelbar wahrnehmbar ist.

Diese verfassungsgerichtlichen Vorgaben im Einzelnen auszugestalten, ist Aufgabe der Gesetzgebung und Rechtsanwendung. In Hinblick auf die Software müssen sich diese sowohl in der technischen Ausgestaltung als auch in den Modalitäten der Anwendung wiederfinden.

Dabei muss Transparenz für die im Einzelfall handelnden Sachbearbeiter:innen geschaffen werden, um nachvollziehen zu können, warum ein KI-gestütztes Entscheidungsunterstützungssystem zu einer bestimmten Einschätzung kommt. Zugleich müssen andererseits die angewandten Kriterien auch im Falle einer späteren gerichtlichen oder datenschutzaufsichtsrechtlichen Nachprüfung erkennbar sein. Dies sollte durch eine umfassende Dokumentation der entscheidungstragenden Faktoren erfolgen.

2. Weitere betroffene Grundrechte

Darüber hinaus ist durch den Einsatz der Software eine Berührung der Schutzbereiche der Menschenwürde (Art. 1 Abs. 1 GG) und des speziellen Diskriminierungsverbots (Art. 3 Abs. 3 GG) denkbar. Verstöße hiergegen sind für die geplanten Einsatzzwecke nicht zu rechtfertigen. Es ist daher durch die Gestaltung der Software und begleitende Maßnahmen wie Schulungen der Sachbearbeiter:innen zu vermeiden, dass die Anwendung des Demonstrators die Schutzbereiche der Art. 1 und Art. 3 GG beeinträchtigt. Zudem kann durch eine ausreichende, den gesetzlichen Anforderungen entsprechende Rechtsgrundlage ein Eingriff in das Fernmeldegeheimnis gem. Art. 10 Abs. 1 Var. 3 GG gerechtfertigt werden.

II. Datenschutzrecht

Neben den verfassungsrechtlichen Vorgaben bestehen einfachgesetzliche datenschutzrechtliche Anforderungen an die Erhebung und Verarbeitung personenbezogener Daten. Diese fußen in erster Linie auf der Datenschutzgrundverordnung (DSGVO) sowie der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr. Diese sog. JI-Richtlinie (JIRL) ist für den hier relevanten Bereich der Gefahrenabwehr und Strafverfolgung durch Behörden wie das BKA maßgeblich. Die DSGVO regelt hingegen primär die Vorgaben für die Datenverarbeitung durch private Stellen. Die Vorgaben der JI-Richtlinie wurden im

BDSG, der StPO und in den Polizeigesetzen des Bundes und der Länder einschließlich des BKAG umgesetzt. Danach müssen die datenschutzrechtlichen Grundprinzipien überwiegend auch von öffentlichen Stellen im Anwendungsbereich der JI-Richtlinie gewahrt werden. Namentlich sind das die Grundsätze der Rechtmäßigkeit, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung sowie Integrität und Vertraulichkeit (§ 47 Nr. 1-6 BDSG).

Für den Software-Einsatz von besonderer Bedeutung ist die Vorgabe des § 54 Abs. 1 BDSG, die vorschreibt: „Eine ausschließlich auf einer automatischen Verarbeitung beruhende Entscheidung, die mit einer nachteiligen Rechtsfolge für die betroffene Person verbunden ist oder sie erheblich beeinträchtigt, ist nur zulässig, wenn sie in einer Rechtsvorschrift vorgesehen ist."

Damit enthält § 54 BDSG einen weiteren Gesetzesvorbehalt (neben dem Verbotsprinzip im Datenschutzrecht), weshalb Behörden im Anwendungsbereich der JI-Richtlinie sich nicht auf bereits bestehende datenschutzrechtliche Ermächtigungsgrundlagen berufen können, um eine automatisierte Entscheidung darauf zu stützen. Insbesondere finden §§ 45 S. 1, 49, 51 BDSG, § 9 BKAG vorliegend keine Anwendung; stattdessen bedarf es einer eigenen gesetzlichen Erlaubnis für automatisierte Entscheidungen. Eine solche Rechtsgrundlage fehlt. § 54 Abs. 1 BDSG setzt jedoch voraus, dass eine Entscheidung ausschließlich automatisiert, also ohne menschliche Kontrolle nach dem Datenverarbeitungsvorgang, ergeht. Die Regelung greift nicht, wenn Entscheidungen durch einen Menschen getroffenen und verantwortet werden – unabhängig davon, ob diesen Entscheidungen eine (automatisierte) Datenverarbeitung vorausgegangen ist oder deren Grundlage bildet.

Im ZMI-Prozess ist jedoch vorgesehen, dass der Demonstrator lediglich der Entscheidungsunterstützung dient. Nach der Bewertung der von dem TMDA übermittelten Inhalte durch den Demonstrator wird das Ergebnis durch menschliche Sachbearbeiter:innen geprüft, die die Strafbarkeit des jeweiligen Inhaltes feststellen müssen, bevor sie die Entscheidung zur Einleitung einer Bestandsdatenabfrage mit dem Ziel, die für ein Strafverfahren örtlich zuständige Stelle zu ermitteln, treffen.

In den Einsatzszenarien des Demonstrators bei ST soll die Software der Analyse großer Datenmengen sowie der Unterstützung der polizeilichen Internetaufklärung dienen. Auch dort

ist vorzusehen, dass unter Berücksichtigung der Ergebnisse der Software menschliche Sachbearbeiter:innen darüber entscheiden, ob weitere strafprozessuale oder gefahrenabwehrrechtliche Maßnahmen ergriffen werden sollen. Daher ist der Einsatz der Software im Einklang mit dem Verbot automatisierter Entscheidungen aus § 54 BDSG denkbar, soweit gewahrt ist, dass die Software lediglich der Unterstützung der Entscheidungsfindung durch einen Menschen dient.

Denkbar erscheint zudem, dass sich Sachbearbeiter:innen von der Software zu einer Entscheidung ‚lenken' lassen. Solche Fälle werden unter dem Begriff ‚automation bias' erforscht. Ein solcher Fall könnte auftreten, wenn die Software einen Straftatbestand fälschlicherweise erkennt bzw. nicht erkennt und die Sachbearbeiter:innen dem unreflektiert folgen und es unterlassen, das Programm prüfend kritisch zu hinterfragen. Eine umfassende Schulung der Sachbearbeiter:innen zum reflektierten Umgang mit der Software kann dieser Problematik vorbeugen.

III. Polizeiliches Eingriffsrecht

Im Rahmen der eingriffsrechtlichen Analyse wurden fünf Szenarien des Software-Einsatzes untersucht. Dies waren die Bewertung von NetzDG-Meldungen hinsichtlich strafbarer Inhalte oder Anhaltspunkte für konkrete Gefahren (Szenario 1), die strafrechtliche Bewertung großer Datensätze (Szenario 2), das Training der KI-Module mit den übermittelten Daten (Szenario 3) sowie der Einsatz der Software zur personenbasierten (Szenario 4) und themenbasierten Recherche (Szenario 5). Zudem wurde untersucht, ob jeweils ein Bedarf zur Rechtsfortbildung besteht.

Zusammenfassend lässt sich festhalten, dass der geplante Software-Einsatz in den Anwendungsszenarien 1 und 2 unter den genannten Umständen rechtmäßig sein kann. Gleichwohl weisen die gesetzlichen Generalklauseln, auf die die Datenverarbeitung gestützt wird, ein hohes Maß an Unbestimmtheit auf. Die Schaffung präziserer Rechtsgrundlagen für die Datenverarbeitung in den Szenarien 1 und 2 erscheint daher nicht als unbedingt erforderlich, aber aus Gründen der Rechtsklarheit als wünschenswert.

Zu Szenario 3 wurde dargelegt, dass die von den TMDA gem. § 3a NetzDG übermittelten Daten als Trainingsdaten für die Software in Frage kämen; die Datenübermittlungspflicht wurde jedoch wegen der zwischenzeitlich ergangenen Rechtsprechung des Verwaltungsgerichts Köln nicht durchgesetzt. Allgemein zeigt sich anhand des Szenarios die Notwendigkeit einer gesetzlichen Regelung für den Umgang staatlicher Stellen mit Trainingsdaten. Dabei besteht ein Zielkonflikt zwischen der Löschpflicht für personenbezogene Daten, die im sicherheitsbehördlichen Bereich regelmäßig besonders sensibel sind, und dem potentiellen Bedarf, anhand von in der Vergangenheit verwendeten Trainingsdaten auch zu einem späteren Zeitpunkt noch die Funktionsweise der damit trainierten Modelle nachvollziehen zu können.

Hinsichtlich der personenbasierten Recherche konnte das Gutachten im Szenario 4 aufzeigen, dass diese jedenfalls nicht im Kontext strafbarer Hassrede zulässig ist (etwas anderes gilt unter Umständen bei terroristischen Aktivitäten). Sollte dieses äußerst eingriffsintensive Vorgehen auch zur Bekämpfung strafbarer Hassrede eingesetzt werden, bedarf es einer gesetzgeberischen Klarstellung dazu. Vergleicht man die Eingriffsintensität der Maßnahme mit dem Gewicht der zu verfolgenden Straftaten bzw. zu schützenden Rechtsgüter, scheint eine Ermächtigung zur personenbasierten Recherche regelmäßig jedoch nicht angemessen zu sein.

Die in Szenario 5 untersuchte themenbasierte Recherche ist im repressiven Bereich derzeit unzulässig; eine gesetzliche Ermächtigung, ohne einen Anfangsverdacht vorauszusetzen, erscheint hingegen nicht sinnvoll möglich zu sein. Die themenbasierte Recherche zu präventiven Zwecken ist hingegen zulässig. Allerdings ist die Datenerhebungsbefugnis des BKA im Rahmen der Zentralstellenfunktion unklar bzw. widersprüchlich geregelt. Hier sollte die Gesetzgebung eine Klarstellung hinsichtlich der Reichweite der zulässigen Datenerhebung treffen.

IV. Handlungsempfehlungen

Zur rechtskonformen Implementierung der im Forschungsprojekt KISTRA entwickelten Software wurden im Rahmen des AP 1.5 Leitlinien entwickelt. Die Beachtung der Leitlinien ersetzt nicht die rechtliche Prüfung der konkreten Zulässigkeit des Software-Einsatzes, sondern dient primär der Orientierung der Endanwender:innen. Sie differenziert in Maßnahmen, die vor

dem Einsatz der Software zu ergreifen sind, während des Einsatzes beachtet werden müssen sowie nach Abschluss des Software-Einsatzes fortgelten. Diese Empfehlungen wurden schließlich zu einer Checkliste mit fünf Punkten verdichtet, um die Implementation in der Praxis zu vereinfachen.[6]

V. Mitwirkungspflichten der Diensteanbieter:innen

Die Mitwirkungspflichten der TMDA bei der Übermittlung von strafbarer Hassrede an die ZMI des BKA sind eine zentrale Änderung des NetzDG im Rahmen der Reform 2021. Dazu werden im Folgenden zunächst die Vorgaben des NetzDG und die hierzu ergangene Rechtsprechung (1.), anschließend der Europäische Digital Services Act (2.) sowie sich aus der Strafbarkeit wegen Unterlassens ergebene Pflichten (3.). beleuchtet.

1. NetzDG

Das NetzDG ist am 01.10.2017 in Kraft getreten und wurde seitdem mehrfach geändert. In seiner Grundkonzeption setzt es bei den sog. Intermediären, also den Betreiber:innen sozialer Netzwerke an. Diese werden verpflichtet, ein Beschwerdesystem einzurichten, das Nutzer:innen verwenden können, um möglicherweise rechtswidrige Inhalte zu melden (§ 3 Abs. 1 NetzDG). Auf die Beschwerde hin ist das soziale Netzwerk dazu verpflichtet, einen „offensichtlich rechtswidrigen Inhalt“ innerhalb von 24 Stunden (§ 3 Abs. 2 Nr. 2 NetzDG) und sonstige rechtswidrige Inhalte innerhalb von sieben Tagen zu entfernen oder den Zugang zu ihnen zu sperren (§ 3 Abs. 2 Nr. 3 NetzDG).

a. Übermittlungspflicht an das BKA gem. § 3a NetzDG

[6] Die Handlungsempfehlungen finden sich im Anhang des Berichts.

Während die NetzDG-Regulierung ab 2017 zunächst auf das Sperren bzw. Löschen rechtswidriger Inhalte setzte, sollten nach der Reform 2021 den Polizeien des Bundes und der Länder Anhaltspunkte zum präventiven und repressiven Vorgehen geliefert werden. Insbesondere wurden Betreiber:innen sozialer Netzwerke verpflichtet, gemeldete Postings an die ZMI im BKA zu übermitteln.

Diese Neuerung ist zum 01.02.2022 in Kraft getreten. Anbieter:innen sozialer Netzwerke müssen nunmehr von Nutzer:innen gemeldete Inhalte daraufhin überprüfen, ob diese eine der in § 3a Abs. 2 NetzDG genannten Katalogstraftaten verwirklichen. Ist dies der Fall, muss der Inhalt entfernt oder der Zugang zu diesem gesperrt werden. Zudem muss der Inhalt an die ZMI übermittelt werden (§ 3a Abs. 3 NetzDG). Die Übermittlung muss auch den „Zeitpunkt, zu dem der Inhalt geteilt oder der Öffentlichkeit zugänglich gemacht" wurde (§ 3a Abs. 4 Nr. 1 NetzDG), den „Nutzernamen" und möglichst die „zuletzt verwendete IP-Adresse einschließlich der Portnummer sowie den Zeitpunkt des letzten Zugriffs" (§ 3a Abs. 4 Nr. 2 NetzDG) enthalten. Zu den praktisch wichtigsten Anwendungsfällen der Übermittlungspflicht dürften die Volksverhetzung (§ 130 StGB) sowie die Bedrohung (§ 241 StGB) mit einem Verbrechen gegen das Leben, die sexuelle Selbstbestimmung, die körperliche Unversehrtheit oder die persönliche Freiheit zählen. Nach der erfolgten Übermittlung an die ZMI wird dort nach dem in Szenario 1 beschriebenen Vorgehen die strafrechtliche Relevanz bewertet, ggf. eine Bestandsdatenauskunft durchgeführt und der Vorgang zur weiteren Bearbeitung an die zuständige Stelle übergeben.

b. Rechtsprechung des Verwaltungsgerichts Köln vom 01.03.2022

Die Übermittlungspflicht gem. § 3a NetzDG findet jedoch keine Anwendung. Mit Beschlüssen vom 01.03.2022[7] gab das Verwaltungsgericht (VG) Köln zwei Anträgen auf einstweiligen Rechtsschutz der Konzerne Google (YouTube) und Meta (Facebook, Instagram) statt. Damit stellte das Gericht vorläufig fest, dass von den Konzernen bis zu einer Entscheidung in der Hauptsache nicht verlangt werden kann, rechtswidrige Inhalte nach den oben geschilderten

[7] Az. 6 L 1277/21; 6 L 1354/21.

Verfahren an das BKA zu übermitteln. Nach Ansicht des Gerichts verstößt die in § 3a NetzDG vorgesehene Übermittlungspflicht gegen die europäische „Richtlinie über den elektronischen Geschäftsverkehr“ (ECRL)[8] und ist daher mangels Vereinbarkeit mit dem Unionsrecht gegenüber den klagenden Unternehmen unanwendbar.

Nach der Richtlinie gilt für die Regulierung von Diensten der Informationsgesellschaft das sog. Herkunftslandprinzip.[9] Daraus folgt, dass nur der jeweilige Staat, in dem ein Unternehmen seinen europäischen Sitz hat, Vorschriften für dieses Unternehmen erlassen kann, auch wenn durch das Unternehmen angebotene Dienste, etwa die sozialen Netzwerke, innerhalb der gesamten Europäischen Union genutzt werden. Da die klagenden Konzerne ihren Sitz in Irland haben, verstoßen deutsche Regulierungsvorschriften, soweit sie den in der ECRL-harmonisierten Bereich betreffen, gegen dieses Prinzip.

2. Digital Services Act

Bei dem Digital Services Act (DSA) handelt es sich um eine Verordnung der Europäischen Union, die zum 17.02.2024 vollständig in Kraft getreten ist und das deutsche NetzDG ersetzt. Damit sollen die zuvor umsetzungsbedürftigen Vorschriften der Art. 12 bis 15 ECRL unionsweit einheitlich konkretisiert werden. Einzelne Vorgaben, die die Regulierung besonders großer Plattformen betreffen, finden bereits zuvor Anwendung. Dies ist dem abgestuften Regelungssystem des DSA mit unterschiedlich intensiven Pflichten für verschiedene „Vermittlungsdienste“, die Informationen übermitteln sowie für die Übermittlung kurzzeitig zwischen- oder dauerhaft speichern, geschuldet. Als EU-Verordnung ist der DSA wie ein nationales Gesetz direkt anwendbar (Art. 288 AEUV) und bedarf – anders als noch die ECRL – keiner Umsetzungsakte.

[8] Richtlinie 2000/31 des Europäischen Parlaments und des Rates vom 08.06.2000 über bestimmte Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“).

[9] VG Köln, Beschl. v. 01.03.2022, Az. 6 L 1277/21, Rn. 152 ff.

Dem Marktortprinzip folgend, gilt der DSA (wie auch schon die DSGVO) für alle Vermittlungsdienste, die Dienstleistungen für Nutzer:innen mit Niederlassung in der EU erbringen – unabhängig davon, wo der jeweilige Dienst seinen Sitz hat. Weitergehende Pflichten gelten für sog. Hosting-Dienste, etwa Webhosting- und Cloud-Angebote sowie Online-Plattformen wie soziale Netzwerke, App-Stores und Online-Marktplätze (Art. 16-32 DSA). Als Online-Plattform gelten Hosting-Dienstanbieter, die im Auftrag ihrer Nutzer:innen Informationen speichern und öffentlich verbreiten, sofern es sich dabei nicht um eine unbedeutende „Nebenfunktion" des eigentlichen Angebots handelt. Dem Erwägungsgrund 14 zufolge soll dies auch Funktionen wie offene Telegram-Gruppen und -Kanäle umfassen. Hinsichtlich des Geltungsbereichs des deutschen NetzDG war diese Frage lange Zeit umstritten, für die Bekämpfung strafbarer Hassrede in der Praxis aber von hoher Relevanz.

a. Löschung illegaler Inhalte

In vielen Punkten ähnelt die Rechtslage nach dem DSA den Vorschriften des NetzDG. So sehen Art. 11, 12 DSA die Einrichtung von Kontaktstellen bzw. Rechtsvertreter:innen für die Kommunikation mit Behörden vor, die ähnlich wie die Zustellungsbevollmächtigten gem. § 5 NetzDG eine effektive Zusammenarbeit mit staatlichen Stellen gewährleisten sollen.

Ähnlich wie das deutsche NetzDG verfolgt der DSA einen „notice and take down"-Ansatz, der auf die Mitwirkung der sozialen Netzwerke setzt. Dafür werden diese verpflichtet, ein funktionierendes Melde- und Abhilfeverfahren (Art. 16 Abs. 1 DSA) zu schaffen, mit dem Nutzer:innen problematische Inhalte beanstanden können. Daraufhin entscheidet die Online-Plattform über die Sperrung bzw. Löschung des fraglichen Inhaltes (Art. 16 Abs. 6 DSA) und informiert die Person, die den Inhalt gemeldet hat, über das Ergebnis der Prüfung (Art. 16 Abs. 5 DSA). Als ‚Ansporn' für die Inhalte-Löschung durch soziale Netzwerke dient die Regelung, dass die dahinterstehenden Konzerne andernfalls ihre Haftungsprivilegierung verlieren (Art. 16 Abs. 3 DSA). Nutzer:innen, deren Inhalt gesperrt wurde, erhalten hierfür eine Erklärung (Art. 17 Abs. 1, 3 DSA); gegen die Entscheidung können sie ein Beschwerdeverfahren bemühen (Art. 21 DSA), wie es auch 2021 als sog. Gegenvorstellungsverfahren in § 3b NetzDG

aufgenommen wurde. In Extremfällen ist auch die temporäre Sperrung von User:innen möglich, die regelmäßig illegale Inhalte veröffentlichen (Art. 23 Abs. 1 DSA).

Dreh- und Angelpunkt der Hassredebekämpfung im DSA ist der Begriff der „illegalen Inhalte". Davon sollen alle Informationen umfasst sein, „die als solche oder durch ihre Bezugnahme auf eine Tätigkeit […] nicht im Einklang mit dem Unionsrecht oder dem Recht eines Mitgliedstaats stehen, ungeachtet des genauen Gegenstands oder der Art der betreffenden Rechtsvorschriften" (Art. 2 lit. h DSA). Der Begriff der illegalen Inhalte ist damit deutlich weiter als der Begriff der „rechtswidrigen Inhalte" in § 1 Abs. 3 NetzDG, der nur Verstöße gegen bestimmte Strafvorschriften umfasst. Mit dem DSA können zukünftig alle Rechtsverstöße gegen europäisches oder mitgliedstaatliches Recht, auch solche gegen das Ehrschutz- oder Urheberrecht, zum Gegenstand des Melde- und Abhilfeverfahrens werden.

b. Begrenzte Übermittlungs- und Überwachungspflichten

Art. 18 DSA sieht ebenfalls eine Übermittlungspflicht der Plattformen an die zuständigen Strafverfolgungs- oder Justizbehörden vor. Eine solche Pflicht soll jedoch nur bestehen, wenn die Plattform vom Verdacht einer Straftat, die eine Gefahr für das Leben oder die Sicherheit von Personen darstellt, Kenntnis erlangt (Art. 18 DSA). Anders als in § 3a NetzDG werden damit ‚typische' Hassrededelikte wie die Volksverhetzung (§ 130 StGB) und Ehrverletzungen (§§ 185-187, 192a StGB) im Normalfall nicht erfasst. Meldungen gem. Art. 18 Abs. 1 DSA sollen zukünftig vom BKA entgegengenommen und dort im Rahmen der gesetzlichen Befugnisse verarbeitet werden. Hier kann auf die für den ZMI-Prozess unter dem NetzDG etablierten Strukturen, insbesondere beim Umgang mit Gefahrenabwehrsachverhalten zurückgegriffen werden.

Eine allgemeine Pflicht der Vermittlungsdienste, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder aktiv nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hindeuten, besteht jedoch nicht (Art. 8 DSA). Auch haften die Diensteanbieter:innen nicht für die auf ihren Angeboten durch Nutzer:innen bereitgestellten Inhalte, sofern sie von deren Rechtswidrigkeit keine Kenntnis haben oder diese Inhalte zügig nach der Zurkenntnisnahme sperren oder löschen (Art. 6 Abs. 1 DSA). Dies gilt auch, sofern

die Anbieter:innen freiwillige Maßnahmen zur Erkennung, Feststellung und Entfernung rechtswidriger Inhalte ergreifen (Art. 7 DSA).

Insgesamt hat die Europäische Union mit dem DSA ein Gesetz zur Plattformregulierung geschaffen, das dem deutschen NetzDG zwar in vielen Punkten ähnelt, aber eine andere Schwerpunktsetzung bei der Bekämpfung von Hassrede setzt. Anstatt wie in §§ 1 Abs. 3, 3 NetzDG nur wenige Strafnormen als „rechtswidrige Inhalte“ zu klassifizieren, die zum Gegenstand eines Melde- und Abhilfe-Verfahrens gemacht werden können, ermöglicht der DSA ein solches für alle „illegalen Inhalte“, die nicht im Einklang mit dem Recht der Europäischen Union oder dem eines Mitgliedsstaats stehen (Art. 2 lit. h DSA). Die Löschpflicht ist unter Umständen also erheblich weiter als im bisher in Deutschland geltenden Recht. Die Pflicht, Inhalte an die Strafverfolgungsbehörden zu übermitteln, wird hingegen in Art. 18 DSA deutlich restriktiver gehandhabt als im – ohnehin praktisch nicht angewandten – § 3a NetzDG.

3. Strafbarkeit wegen Unterlassens

Weitergehende Verpflichtungen der Diensteanbieter:innen könnten sich aus den Vorschriften über die Strafbarkeit wegen Unterlassens ergeben. Allgemein gilt, dass sich unter bestimmten Umständen derjenige strafbar machen kann, der die Verwirklichung eines Straftatbestands nicht abwendet, „wenn er rechtlich dafür einzustehen hat, daß der Erfolg nicht eintritt, und wenn das Unterlassen der Verwirklichung des gesetzlichen Tatbestandes durch ein Tun entspricht“ (§ 13 Abs. 1 StGB). Im Kontext der Verbreitung von Hassrede kommt dabei primär eine Beihilfe durch Unterlassen der Löschung des jeweiligen Inhalts durch die Mitarbeiter:innen der TMDA in Betracht. Dies würde jedoch das Bestehen einer Garantenpflicht voraussetzen, die sich jedenfalls nicht aus § 10 TMG bzw. Art. 6 Abs. 1 DSA ergibt. Ob eine Garantenpflicht aus der Beherrschung des Sozialen Netzwerks als „Gefahrenquelle“ besteht, ist fraglich, würde jedoch allenfalls ab positiver Kenntnis – in der Regel durch die Meldung von Nutzer:innen – in Frage kommen. Damit ergeben sich aus den Vorschriften zur Unterlassensstrafbarkeit keine weitergehenden Pflichten als aus den Regelungen des NetzDG bzw. Digital Services Act.

D. Fazit und Ausblick

Abschließend werden im Folgenden die Ergebnisse des Projektes zusammengefasst und ein kurzer Ausblick auf den weiteren Forschungsbedarf gegeben.

I. Zusammenfassung der Ergebnisse

Das im Projekt angefertigte Gutachten konnte aufzeigen, in welchem Umfang der geplante Einsatz der Klassifizierer-Software zur Erkennung bestimmter Formen strafbarer Hassrede sowie von Anzeichen für mögliche Gefahrenabwehrsachverhalte in Grundrechte, insbesondere in das Recht auf informationelle Selbstbestimmung, eingreift. Ob dies im jeweiligen Anwendungsfall gerechtfertigt werden kann, hängt von der Intensität des Grundrechtseingriffs sowie den tatsächlichen Anhaltspunkten für das Bestehen eines strafrechtlichen Tatverdachts bzw. des Vorliegens einer polizeirechtlichen Gefahr ab. Zudem ist beim Einsatz der Software die Wertung des § 54 BDSG zu beachten, nach welchem lediglich eine Entscheidungsunterstützung für menschliche Sachbearbeiter:innen, nicht jedoch eine automatisierte Einzelentscheidung zu Lasten der Betroffenen zulässig ist. Auch wenn sich vielfältige Einsatzszenarien der Software aufgrund bestehender Generalklauseln zur Datenerhebung und -verarbeitung realisieren lassen, erscheint es perspektivisch geboten, den Einsatz von Methoden maschinellen Lernens zur Datenauswertung durch das BKA spezialgesetzlich zu regeln. Dabei sollte ebenfalls normiert werden, wie mit der langfristigen Speicherung von Trainingsdaten für die eingesetzte Klassifizierer-Software umzugehen ist. Solange keine spezialgesetzliche Ermächtigung vorliegt, sind in der praktischen Gestaltung des Software-Einsatzes Maßnahmen zu ergreifen, um die Intensität der damit verbundenen Grundrechtseingriffe möglichst gering zu halten.

Die Rechtslage hinsichtlich der Mitwirkungspflichten der TMDA an der Strafverfolgung hat sich während des Projektverlaufs aufgrund aktueller Entwicklungen in der Gesetzgebung und Rechtsprechung fundamental verändert. Während zu Projektbeginn im Juli 2020 noch das „alte“ NetzDG galt, das lediglich eine Sperr- bzw. Löschpflicht der sozialen Netzwerke für rechtswidrige Inhalte vorsah, wurden die Mitwirkungspflichten durch das 2021 beschlossene Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität erheblich ausgeweitet. Die ab 01.02.2022 geltende Übermittlungspflicht für strafbare Inhalte an das BKA (§ 3a NetzDG) wurde aufgrund der am 01.03.2022 verkündeten Beschlüsse des VG Köln nicht angewandt. Nach Abschluss des Projekts tritt

das deutsche NetzDG zum 17.02.2024 vollständig außer Kraft. Viele der im NetzDG enthaltenen Regelungen werden jedoch in ähnlicher Weise unter dem ab dem 17.02.2024 geltenden DSA fortgeführt.

II. Weiterer Forschungsbedarf

Im Folgenden sollen einige Möglichkeiten weitergehender Forschung hinsichtlich der infrastrukturellen Verpflichtungen der TMDA zur Bekämpfung strafbarer Hassrede diskutiert werden. Dabei sollen die jüngste Rechtsprechung hinsichtlich der Löschung vergleichbarer Inhalte (1.) und die gesetzgeberischen Pläne hinsichtlich sog. Accountsperren (2.) kurz thematisiert werden.

1. Pflicht zur Löschung vergleichbarer Inhalte

Wie oben dargelegt, bestand bisher nach dem NetzDG und besteht zukünftig nach dem DSA eine Pflicht der TMDA, rechtswidrige Inhalte nach der Meldung durch Nutzer:innen zu sperren bzw. zu löschen. Strafbare Hassrede wird jedoch häufig nicht nur von einzelnen Nutzer:innen sozialer Netzwerke veröffentlicht, sondern von einer Vielzahl an Personen weiterverbreitet. Dabei kommt es vor, dass dies nicht nur für die jeweiligen Share/Like-Funktion unter Einbettung des ursprünglichen Inhalts erfolgt, sondern Hassrede in Form von Bildern („Sharepics“), Videos o.ä. von Nutzer:innen herunter- und erneut hochgeladen wird. Dadurch besteht keine direkte digitale Verweisung zwischen gleichartigen Hassrede-Inhalten. Vor diesem Hintergrund wird in Rechtswissenschaft und -politik diskutiert, ob die Betreiber:innen sozialer Netzwerke verpflichtet sind, wort- und/oder sinngleiche Inhalte zu löschen, nachdem ein vergleichbarer Inhalt erfolgreich beanstandet wurde.

Mit seiner Entscheidung in der Rechtssache *Glawischnig-Piesczek v. Facebook Ireland Limited* entschied der EuGH, dass das Unionsrecht den Mitgliedstaaten nicht verbietet, Hosting-Anbieter zur weltweiten Sperrung bzw. Löschung wortgleicher rechtswidriger Inhalte sowie

unter bestimmten Umständen auch sinngleicher Inhalte zu verpflichten.[10] Viele Details zu dieser Thematik blieben in der Entscheidung jedoch offen und sind der weiteren Auslegung der nationalen Rechtsprechung und -wissenschaft überlassen. Auf nationaler Ebene sind erstinstanzlich ähnliche Entscheidungen ergangen, die die Betreiberin der Facebook-Plattform zum Vorgehen gegen persönlichkeitsrechtsverletzende Darstellungen unabhängig von der individuellen Meldung eines bestimmten Inhalts verpflichten.[11] Die Rechtsprechung zur Pflicht der TMDA, gegen vergleichbare persönlichkeitsrechtsverletzende Inhalte vorzugehen, ist mithin erst im Entstehen begriffen. Ob sich diese ohne weiteres auf strafbare Hassrede übertragen lässt und in welchem Umfang derartige Pflichten – gerade vor dem Hintergrund der Privilegierung des § 10 TMG bzw. Art. 6 Abs. 1 DSA – bestehen können, sollte Gegenstand weiterer rechtswissenschaftlicher Forschung sein.

2. Einführung eines Verfahrens zur Anordnung von Accountsperren

Als weiteren Schritt der Bekämpfung strafbarer Hassrede plant die Bundesregierung derzeit die Einführung eines Gesetzes gegen digitale Gewalt und legte hierzu im April 2023 ein erstes Eckpunktepapier vor.[12] Neben weitergehenden Auskunftsrechten zur privaten Rechtsdurchsetzung gegen individuelle Rechtsverstöße sieht das Gesetz einen Anspruch auf richterlich angeordnete Sperrungen von Accounts vor. In Fällen wiederholter Persönlichkeitsrechtsverletzungen soll der:die Betroffene gegenüber den jeweiligen Diensteanbieter:innen erwirken können, dass der Account, über den die Rechtsverletzungen erfolgen, gesperrt wird. Anknüpfungspunkte für die rechtswissenschaftliche Forschung ergeben sich hier einerseits zu der Frage, inwiefern derartige nationale Regelungen neben der EU-Verordnung des Digital Services Acts kompetenzrechtlich möglich sind. Andererseits sollte auch das Zusammenspiel verschiedener infrastruktureller Pflichten – etwa des Beschwerde- und Abhilfeverfahrens nach dem DSA, der Übermittlungspflicht bestimmter Inhalte an

[10] Europäischer Gerichtshof, Urteil vom 03.10.2019, Az. C-18/18, Rn. 53.

[11] LG Frankfurt am Main, Urteil vom 08.04.2022, Az. 2-03 O 188/21; LG Bonn, Beschluss vom 05.07.2023, Az. 9 O 130/23.

[12] *Bundesministerium der Justiz*, Eckpunkte des Bundesministeriums der Justiz zum Gesetz gegen digitale Gewalt, 2023.

Polizeibehörden sowie perspektivisch des Einsatzes gerichtlich angeordneter Accountsperren – wissenschaftlich untersucht werden.

E. Anhang

Die Erkenntnisse aus dem Teilvorhaben haben Eingang in diverse Veröffentlichungen und Vorträge gefunden.

I. Publikationen

Die folgenden Publikationen von Jun.-Prof. Dr. Sebastian Golla und Marius Kühne sind im Verlauf des Projekts entstanden:

1. Golla, Sebastian: Schwärme und Cybermobbing – Gruppenbezogenes Strafrecht in der virtuellen Welt, in: Köhler, Ben; Koch, Stefan (Hrsg.): Schwärme im Recht, 2022, S. 77-88.
2. Golla, Sebastian: Grundrechtliche Eingriffe durch Internetauswertungen, in: Golla, Sebastian; Pelzer, Robert (Hrsg.): Themenheft Open Source Intelligence, Polizei.Wissen, Heft 9, 2022, S. 9-12.
3. Kühne, Marius: Bitte melden! Rechtliche und praktische Tücken der NetzDG-Meldepflicht, in: JuWissBlog Nr. 9/2022 v. 31.01.2022, https://www.juwiss.de/9-2022/.
4. Kühne, Marius: Hass regeln? Schwierigkeiten der Rechtsdurchsetzung gegen Hassrede im Internet, in: Golla, Sebastian; Pelzer, Robert (Hrsg.): Themenheft Open Source Intelligence, Polizei.Wissen, Heft 9, 2022, S. 21-24.
5. Kühne, Marius: DSA statt NetzDG –Was ändert sich bei der Bekämpfung von Hassrede in sozialen Netzwerken?, in: JuWissBlog Nr. 49/2022 v. 04.08.2022, https://www.juwiss.de/49-2022/.
6. Kühne, Marius: Bloß nicht hetzen lassen! Die (polizeiliche) Bekämpfung von Hassrede im Internet, in: Feltes, Thomas; Klaas, Kathrin; Thüne, Martin: Sammelband „Digitale Polizei“, 2022, S. 299-316.

II. Vorträge

Erkenntnisse aus der Untersuchung fanden als Lehrbeispiele schließlich Eingang in die Vorlesungen und Seminare an der Ruhr-Universität Bochum.

- Vortrag zum Schwarmstrafrecht auf der Tagung „Schwärme im Recht“ am Max-Planck-Institut für ausländisches und internationales Privatrecht am 30.6.2022 in Hamburg.
- Vortrag „Künstliche Intelligenz in Strafverfolgung und Gefahrenabwehr“ auf der Mitgliederversammlung des Vereins zur Förderung der Rechtswissenschaft e.V. am 23.11.2023 in Bochum.

III. Handlungsempfehlungen

Die nachfolgenden Leitlinien sollen die rechtskonforme Implementierung der im Forschungsprojekt KISTRA entwickelten Software unterstützen. Die Beachtung der Leitlinien ersetzt nicht die rechtliche Prüfung der konkreten Zulässigkeit des Software-Einsatzes. Die Achtung der datenschutz- und eingriffsrechtlichen Vorgaben ist jeweils durch die handelnden Sachbearbeiter:innen bzw. ihre Vorgesetzten sicherzustellen. Kann dies nicht gewährleistet werden, ist der Einsatz der Software einzustellen.

1. Vor dem Einsatz der Software

a. Die zuständigen Sachbearbeiter:innen sollen über die rechtlichen Grundlagen der Datenerhebung und -auswertung im Allgemeinen sowie des Einsatzes der im Projekt entwickelten Software im Besonderen aufgeklärt werden. Ihnen soll bekannt sein, dass jeder Schritt der Erhebung und -verarbeitung personenbezogener Daten einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung bewirkt. Eingriffe müssen auf eine gesetzliche Grundlage gestützt werden. Maßgeblich sind gesetzliche Vorschriften des Netzwerkdurchsetzungsgesetzes (NetzDG) bzw. des Digital Services Acts (DSA), des Bundesdatenschutzgesetzes (BDSG), des Bundeskriminalamtsgesetzes (BKAG) sowie der Strafprozessordnung (StPO).

aa. Das Konzept des Eingriffsgewichts bei staatlichen Eingriffen in das Grundrecht auf informationelle Selbstbestimmung soll erlernt und verstanden werden. Die Sachbearbeiter:innen sollen einschätzen können, welche Faktoren das Eingriffsgewicht bei der Datenerhebung erhöhen und wie sich die automatisierte Auswertung der jeweiligen Daten, insbesondere durch Methoden des maschinellen Lernens bzw. sog. Künstlicher Intelligenz, darauf auswirkt.

bb. Die Problematik möglicher Diskriminierungsrisiken bei automatisierten Datenauswertungen soll bekannt sein. Die Sachbearbeiter:innen sollen, ggf. durch Schulungen, für die Risiken des Software-Einsatzes hinsichtlich der ungleich präzisen Erkennung bestimmter strafbarer Inhalte sowie bzgl. der eigenen Prüfpflicht der softwaregestützten Ergebnisse und möglicher Wahrnehmungsverzerrungen (automation / confirmation bias) dabei sensibilisiert werden.

cc. Datenschutzrechtliche Konzepte wie das Verbotsprinzip, der Grundsatz der Zweckbindung und das Verbot automatisierter Einzelentscheidungen sollen erlernt und verstanden werden. Sachbearbeiter:innen sollen mit dem Ziel geschult werden, die Software lediglich entscheidungsunterstützend und zur Realisierung des Zweckes der Datenerhebung einzusetzen. Dazu ist ein grundlegendes Verständnis für die ‚Fähigkeiten' der Software notwendig.

b. Der:Die Datenschutzbeauftragte der Institution soll frühzeitig eingebunden werden. Gemeinsam mit ihm:ihr wird ein Datenschutzkonzept entworfen und geprüft, ob eine Datenschutzfolgeabschätzung erforderlich ist.

c. Der Einsatz der Software soll dokumentiert und idealerweise wissenschaftlich begleitet werden. Die Dokumentation dient auch der Umsetzung der datenschutzrechtlichen Benachrichtigungspflichten (vgl. dazu 3.d).

2. Während des Einsatzes der Software

a. Die Sachbearbeiter:innen sollen stets wissen, ob sie im Bereich der Gefahrenabwehr oder Strafverfolgung tätig werden und auf Grund welcher Rechtsgrundlagen ihr Handeln erfolgt.

b. Die Sachbearbeiter:innen sollen stets wissen, aus welcher Quelle die Daten stammen, die ausgewertet werden (Übermittlung von TMDA/Zivilgesellschaft; Art der polizeilichen Datenerhebung, z.B. Sicherstellung/Beschlagnahme, OSINT-Recherche). Auch sollen sie erkennen können, ob besondere

Kategorien personenbezogener Daten, aus denen etwa die politische Meinung, weltanschauliche Überzeugung, sexuelle Orientierung oder gesundheitliche Verfassung der Person hervorgeht, einbezogen werden.

c. Die Sachbearbeiter:innen sollen beim Einsatz der Software möglichst erkennen können, an welche Merkmale (Begriffe, Formulierungen, Symbole) die Software die strafrechtliche Bewertung anknüpft. Dies kann durch farbliche Hervorhebungen o.ä. erfolgen.

d. Bei der Prüfung der strafrechtlichen Relevanz sollen den Sachbearbeiter:innen nur die für die Prüfung erforderlichen Datenpunkte angezeigt werden. Weitere personenbezogene Angaben, etwa Username und Profilbild, sollen nach Möglichkeit zunächst ausgeblendet sein, sodass die Wahrnehmung dieser Daten durch die Sachbearbeiter:innen einen zusätzlichen Arbeitsschritt erfordert. Damit verbunden soll eine Reflektion stattfinden, ob es für die Prüfung notwendig ist, diese Daten einzubeziehen.

e. Es soll eine Dokumentation stattfinden, in der u.a. festgehalten wird, in welchen Fällen die Software eingesetzt wird und ob die Sachbearbeiter:innen den Empfehlungen der Software bei der strafrechtlichen Bewertung folgen. Dabei soll auch der ‚Trainingsstand' der verwendeten Software dokumentiert werden.

3. Nach Abschluss des Einsatzes der Software

a. Nach Feststellung der örtlichen/sachlichen Zuständigkeit sollen der Vorgang an die jeweilige Stelle abgegeben und die dazugehörigen Daten in der Regel gelöscht werden. Die Entscheidung, Daten in Ausnahmefällen weiterhin zu speichern, soll schriftlich unter Verweis auf die jeweiligen Rechtsgrundlagen begründet werden.

b. Wenn geprüfte Inhalte als Trainingsdaten für die Software genutzt werden sollen, sollen alle nicht notwendigen Personenbezüge entfernt bzw. die Daten anonymisiert werden. Die Nutzung als Trainingsdaten stellt einen neuen Verarbeitungszweck dar, dessen Rechtmäßigkeit erneut geprüft werden muss.

c. Es soll regelmäßig geprüft werden, ob der Einsatz der Software weiterhin notwendig und zweckdienlich ist. Wenn möglich, soll die Nutzung der Software wissenschaftlich evaluiert werden.

d. Es soll bereits mit dem Einsatz der Software ein System geschaffen werden, wie etwaige Benachrichtigungspflichten und weitere Betroffenenrechte in der Praxis umgesetzt werden können.

4. Checkliste

O Rechtliche Grundlagen für Handeln sind bekannt.

O Schulung zu Eingriffsgewicht und Diskriminierungsrisiken ist erfolgt.

O Datenschutzbeauftragte:r wurde einbezogen, Datenschutzkonzept liegt vor.

O Datenquellen für Auswertung und Funktionsweise der Software sind bekannt.

O Software-Einsatz wird dokumentiert und evaluiert.