

Mit künstlicher Intelligenz auf Verbrecherjagd

Christian Rückert

2021-01-22T11:53:11

Zur Fahndung nach den Beteiligten am Sturm auf das US-amerikanische Kapitol werden nach [Medienberichten](#) wohl auch Gesichtserkennungstechnologien eingesetzt, die teilweise auf künstlicher Intelligenz beruhen. Der Einsatz solcher – dem Bereich der automatisierten Open Source Intelligence-Maßnahmen zuzuordnenden – Techniken ist nach amerikanischem (Verfassungs-)Recht umstritten. Nach deutschem Recht wäre er derzeit unzulässig. Die Einführung einer entsprechenden Rechtsgrundlage erfordert aufgrund ethischer, technischer und menschenrechtlicher Implikationen eine intensive Debatte auf gesetzgeberischer Ebene.

Black Lives Matter, Sturm auf das Kapitol und Soziale Medien

Die systematische Überwachung und Auswertung (teil-)öffentlich zugänglicher Internetquellen zur Strafverfolgung und Gefahrenabwehr ist in den USA bereits weit verbreitet. Im Fokus der Ermittler stehen hier meist soziale Medien. Dort können die Behörden vor allem auf Bild- und Videomaterial zugreifen, das die Tatverdächtigen selbst oder Dritte hochladen. Gerade bei medienwirksamen Ereignissen – wie dem Sturm auf das Kapitol – wird dieses Material vielfach „geteilt“. Zum Auffinden und zur Auswertung der Social-Media-Daten werden auch moderne, oftmals auf künstlicher Intelligenz oder anderen selbstlernenden Technologien basierende Datenauswertungsprogramme, wie zum Beispiel Gesichtserkennungssoftware, verwendet. So griffen die US-Behörden zu Fahndungszwecken bei den sogenannten ‚Black Lives Matter‘-Demonstrationen in den USA auf die [Überwachung von Aktivitäten in sozialen Medien](#) und den Einsatz von [Gesichtserkennungssoftware](#) zurück. Auch bei der Aufklärung von Straftaten und der Suche nach den Tätern beim Sturm auf das Kapitol am 6. Januar werten US-Bundesbehörden Bilder und Videos aus sozialen Medien aus. Ob dabei ebenfalls KI-basierte Gesichtserkennungstechnologie eingesetzt wird, lassen die US-Bundesbehörden auf Medienanfragen [bislang unkommentiert](#), obwohl lokale Polizeibehörden dies [bereits eingeräumt](#) haben. Die gern von US-Behörden genutzte Gesichtserkennungs-App „Clearview“ verzeichnete am Tag des Sturms auf das Kapitol einen [Suchanfragenanstieg um 26%](#), was zumindest einen starken Hinweis auf eine behördliche Nutzung zur Identifikation von Straftätern im Zusammenhang mit dem Angriff liefert. Auch in der Vergangenheit haben US-Behörden wie das FBI, die DEA (Drogenfahndung) oder die ICE (Grenz- und Zollbehörde) [wiederholt](#) auf [automatisierte Gesichtserkennungssoftware](#) zurückgegriffen.

KI, Gesichtserkennung und das „Fourth Amendment“

Die [US-amerikanische Debatte um die Zulässigkeit solcher Technologien](#) – insbesondere, wenn sie auf künstlicher Intelligenz oder anderen selbstlernenden Verfahren basieren – dreht sich hauptsächlich um den vierten Verfassungszusatz, das sogenannte ‚Fourth Amendment‘. Dieser für das amerikanische Strafverfahrensrecht immens bedeutsame [Verfassungszusatz](#) schützt die Bevölkerung vor willkürlichen polizeilichen Maßnahmen und begrenzt die Zulässigkeit von Ermittlungsmaßnahmen, wie Hausdurchsuchungen und Telekommunikationsüberwachung. Daneben wird auch oft der [erste Verfassungszusatz](#) („freedom of speech“) ins Spiel gebracht. Dabei geht es hauptsächlich um [sogenannte ‚Chilling Effects‘](#), also die Annahme, dass Bürger/innen ihre Grundrechte auf Meinungsäußerungs- und Versammlungsfreiheit weniger wahrnehmen, wenn sie davon ausgehen müssen, nicht nur überwacht, sondern später mittels (KI-basierter) Gesichtserkennung auch identifiziert zu werden und daher persönliche Nachteile zu befürchten haben.

Einsatz automatisierter Open Source Intelligence in Deutschland

Die Erhebung und Auswertung von Bild- und Videomaterial mittels selbstlernender Software aus öffentlich zugänglichen Internetquellen ist ein Unterfall der sogenannten ‚Open Source Intelligence‘ (OSINT). Dieser Begriff fasst Ermittlungsmethoden zusammen, bei denen Daten und Informationen aus öffentlich zugänglichen Quellen erhoben, zusammengetragen und ausgewertet werden. Die Methode besteht dabei aus zwei Schritten. In einem ersten Schritt werden die Daten aus dem Internet (z.B. Soziale Medien, Foren, Verkaufsplattformen, Internetseiten) erhoben. Hierzu kommen in der Regel sogenannte [Web-Scraper](#) (auch Web-Crawler genannt) zum Einsatz. Das sind [Programme](#), die das Internet selbsttätig nach bestimmten Informationen durchsuchen, die entsprechenden Daten herunterladen und diese in großen Datenbanken speichern. Der zweite Schritt besteht aus der Auswertung der Daten. Da hier regelmäßig sehr große Datenmengen zusammenkommen, wird auf Auswertungssoftware und Data Mining-Methoden zurückgegriffen. Der Einsatz selbstlernender Technologien, wie [Machine Learning, Deep Learning oder künstliche Intelligenz bietet sich an](#), weil diese Programme die Datenanalyse – so zumindest versprechen es die Hersteller – noch schneller und effizienter durchführen und noch mehr Informationen aus den Daten generieren können, als dies mit weniger fortgeschrittenen Methoden möglich ist. Der Vorteil liegt darin, dass diese Programme sich während der Analyse von Datensätzen „selbst trainieren“ und somit bei nachfolgenden Analysen Zusammenhänge in den Daten schneller und/oder genauer erkennen.

Auch in Deutschland werden die beschriebenen Methoden bereits durch die Polizei eingesetzt, beziehungsweise deren Einsatz erforscht: Neben dem [Einsatz von Gesichtserkennungssoftware zur Auswertung von Videoüberwachungsbildern](#)

öffentlicher Plätze geht es beispielsweise um die [Kriminalitätsprognose](#) (sog. „predictive policing“), [Nachverfolgung von Zahlungsströmen in Kryptowährungssystemen](#), die [Erhebung und Auswertung von Daten aus Online-Foren](#) und [Sozialen Medien](#) (sog. SOCMINT), die [Strafverfolgung im sogenannten Darknet](#) und die [Auswertung von sichergestellten kinderpornografischen Bildern und Videos](#).

Zulässigkeit nach deutschem Verfassungs- und Strafprozessrecht

Die Bewertung, ob und gegebenenfalls unter welchen Voraussetzungen der Einsatz von automatisierten OSINT-Methoden zur Verfolgung von Straftätern in Deutschland zulässig ist, erfordert eine mehrschichtige Betrachtung. Es muss zwischen Verfassungs- und Strafprozessrecht unterschieden werden, wobei die strafprozessuale Bewertung stark von den verfassungsrechtlichen Vorwertungen geprägt ist.

Verfassungsrecht: Vorbehalt des Gesetzes und Recht auf informationelle Selbstbestimmung

Aufgrund des aus Art. 20 Abs. 3, 1 Abs. 3 GG abzuleitenden verfassungsrechtlichen Prinzips des Vorbehalts des Gesetzes, erfordert jeder Grundrechtseingriff durch staatliche Behörden eine Rechtsgrundlage. Die Rechtsgrundlagen für strafprozessuale Grundrechtseingriffe finden sich in der Strafprozessordnung (StPO). Auch die Erhebung und Auswertung von öffentlich zugänglichen personenbezogenen Daten stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG dar. Bei [automatisierter Datenerhebung](#) und -auswertung gilt dies nach der Rechtsprechung des BVerfG immer. Bei der [manuellen Datenerhebung](#) (wenn also ein/e Polizeibeamte/r selbst die Information händisch recherchiert) soll dies dagegen nur dann der Fall sein, wenn die Daten und Informationen „gezielt zusammengetragen, gespeichert und gegebenenfalls unter Hinzuziehung weiterer Daten ausgewertet werden und sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt“. Zur Begründung führt das [BVerfG](#) – recht vage – aus, dass das Recht auf informationelle Selbstbestimmung auch die informationellen Schutzinteressen desjenigen schützen würden, der sich in die Öffentlichkeit begibt. Weder aus dem Schritt in die Öffentlichkeit noch aus der Kenntnis des Überwachtwerdens kann ein Einverständnis in die Datenerhebung hergeleitet werden. Dass die gemachte Unterscheidung zwischen manueller und automatisierter Datenerhebung angesichts dieser Begründung nicht nachvollziehbar ist, ist für den hier betrachteten Bereich nicht relevant, weil es bei automatisierten OSINT-Methoden stets um [automatisierte Datenerhebungen und/oder -auswertungen](#) geht. Schließlich ist zu beachten, dass nach neuerer [Rechtsprechung des BVerfG](#) nicht nur ein Grundrechtseingriff für diejenigen Personen anzunehmen ist, bei denen die automatische Auswertung einen „Treffer“ ergibt, sondern auch für alldiejenigen, deren Daten in die Suche und Auswertung einbezogen wurden, gegenüber denen aber, mangels „Treffer“,

keine weiteren Maßnahmen ergriffen werden. Demnach ist für die hier betrachteten OSINT-Methoden eine strafprozessuale Rechtsgrundlage erforderlich.

Keine Rechtsgrundlage in der Strafprozessordnung

[Eine spezifische Rechtsgrundlage für OSINT-Methoden enthält die StPO bislang nicht](#). Eine gewisse sachliche Nähe besteht höchstens zur Rasterfahndung ([§ 98a StPO](#)) und zum justiziellen Datenabgleich ([§ 98c StPO](#)). Letztere Vorschrift regelt jedoch nur den maschinellen Abgleich von Daten, über welche Polizei und Staatsanwaltschaften bereits verfügen und gibt dementsprechend keine Befugnis zur Neu-Erhebung von Daten.

Auch § 98a StPO „passt“ nicht. Zwar gibt es Gemeinsamkeiten: § 98a StPO erlaubt die Erhebung von abzugleichenden Daten von anderen „speichernden Stellen“ (Abs. 2) und hat zum Ziel, einen Tatverdächtigenkreis aus einer großen Menge von einbezogenen Personen herauszufiltern. Die Maßnahmen richten sich also gezielt gegen eine große Gruppe nicht tatverdächtiger Personen. Es bestehen jedoch so erhebliche Unterschiede zwischen automatisierten OSINT-Methoden und Rasterfahndung, dass eine Subsumtion unter § 98a StPO im Ergebnis nicht möglich ist. Während bei § 98a StPO ausschließlich Daten Verwendung finden, die bereits in Datenbanken (ggf. außerhalb von Polizei und Justiz) gespeichert sind, werden bei OSINT im Scraping-Schritt neue Daten aus dem Internet erhoben. Auch richtet sich § 98a StPO vor allem auf den Abgleich von nicht öffentlich zugänglichen Daten wie KFZ-Zulassungsregistern, Kundendateien von Stromanbietern, Melderegistern etc., während OSINT – wie der Name schon sagt – auf öffentlich zugängliche Daten des Internets beschränkt ist. Die enorme Datenmenge, die hierbei zusammenkommt (z.B. hat die Gesichtserkennungs-App Clearview [laut Medienberichten](#) durch gezieltes Scraping bereits über 3 Milliarden Bilder von Personen zusammengetragen) liefert ein weiteres Argument gegen eine Subsumtion unter § 98a StPO.

Die Datenmenge, die bei automatisierten, insbesondere KI-basierten OSINT-Maßnahmen, wie der Auswertung von Bildern und Videos der Angriffe auf das Kapitol unter anderem aus sozialen Medien verarbeitet werden, stellt jede klassische Rasterfahndung in den Schatten. Die technologischen Möglichkeiten, die hierfür heute zur Verfügung stehen, hätte sich der Gesetzgeber von 1992 nicht träumen lassen. Insbesondere die KI-basierten OSINT-Maßnahmen zur Massendatenerhebung und -auswertung geben der Intensität der mit ihr verbundenen, massenhaften Grundrechtseingriffe (sog. Streubreite der Maßnahme) ein völlig anderes Gepräge. Daher steht auch der verfassungsrechtliche [Wesentlichkeitsvorbehalt](#) einem „Hineinquetschen“ der automatisierten OSINT-Maßnahmen in § 98a StPO entgegen. Hiernach muss der parlamentarische Gesetzgeber selbst über alle „wesentlichen“ Grundrechtsfragen entscheiden. Angesichts der großen Eingriffsintensität und der neuen Dimension an Massendatenerhebung und -auswertung muss sich der Gesetzgeber mit der Zulässigkeit und den Grenzen einer solchen Maßnahme auseinandersetzen. Aus denselben Gründen (hohe Eingriffsintensität aufgrund der großen Streubreite, Wesentlichkeitsvorbehalt) können die Maßnahmen auch nicht auf die sogenannten Ermittlungsgeneralklauseln der §§ 161, 163 StPO gestützt werden, da diese [nur für](#)

[„geringfügige“ Grundrechtseingriffe](#) herangezogen werden können (die §§ 161, 163 StPO können allerdings nach derzeit h.M. Rechtsgrundlage für „manuelle“ OSINT-Maßnahmen wie sog. Online-Streifen sein).

Verbot „kafkaesker“ Maschinenentscheidungen

Wie gezeigt, gehen mit automatisierten OSINT-Methoden erhebliche Grundrechtseingriffe einer Vielzahl von Betroffenen einher. Dies gilt in besonderem Maße für selbstlernende Systeme, wie zum Beispiel KI-basierte Gesichtserkennungssoftware. Nach deutschem Recht ist der Einsatz solcher Methoden zur Strafverfolgung mangels einschlägiger Rechtsgrundlage in der StPO derzeit unzulässig. Bei der notwendigen gesetzgeberischen Debatte über die Einführung einer Eingriffsbefugnis für automatisierte, insbesondere selbstlernende und KI-basierte OSINT-Methoden müssen – neben der bereits beschriebenen großen Eingriffsintensität dieser Maßnahmen aufgrund der massenhaften Betroffenheit von Grundrechtsträger/innen – vor allem zwei Aspekte berücksichtigt werden:

Europarecht: Verbot der nachteiligen Entscheidungen „allein“ durch Maschinen

Da OSINT-Methoden sowohl der Eingrenzung des Tatverdächtigenkreises (häufiger) als auch dem Schuldnachweis dienen können (seltener, jedoch beim hier eingangs geschilderten Beispielsfall der Auswertung von Bildern und Videos des Angriffs auf das Kapitol durchaus denkbar), sind an die Ergebnisse der maschinengesteuerten Massendatenerhebung und -auswertung in aller Regel negative Rechtsfolgen für die Betroffenen geknüpft (weitere grundrechtsbeeinträchtigende Ermittlungsmaßnahmen oder sogar die Verhängung einer Kriminalstrafe). Dies wirft die grundlegende ethische wie menschenrechtliche Frage auf, ob Entscheidungen über das Schicksal von Menschen in die Hände von „denkenden“ Maschinen gelegt werden dürfen. Europarechtlich ist dieses Problem in [Art. 11 der Richtlinie 2016/680/EU](#) (als „Schwestervorschrift“ zu [Art. 22 DSGVO](#)) geregelt, welche im deutschen Recht (allerdings nicht vollständig) in [§ 54 BDSG](#) umgesetzt ist. Hiernach ist es verboten, Entscheidungen, welche mit nachteiligen Rechtsfolgen für Personen verbunden sind, allein durch Maschinen treffen zu lassen. Weiterer Diskussion bedarf hier allerdings die Frage, [wann eine Entscheidung „allein“ durch eine Maschine getroffen wird](#). Die Problematik berührt aber auch die Menschenwürdegarantie aus Art. 1 Abs. 1 GG, Art. 1 EU-GRCh, sodass die Grenzen nicht allein durch Art. 11 Richtlinie 2016/680/EU und § 54 BDSG gezogen werden.

Irren ist nicht nur menschlich

Weiterhin müssen die [grundlegenden technischen Probleme](#) beim Einsatz [von selbstlernenden Systemen](#) und [künstlicher Intelligenz](#) in die Diskussion um das „Ob“ und „Wie“ des Einsatzes solcher Technologien einbezogen werden. Hierzu gehören vor allem Sorgen um die Replizierung menschlicher Fehler bei der Informationsverarbeitung (Stichwort Bias), hieraus erwachsende Probleme der Diskriminierung, notwendige Richtigkeitsgewähr, Überschätzung der Verlässlichkeit der Datenverarbeitung sowie fehlende Transparenz und Nachvollziehbarkeit der

angewendeten Methoden („[Blackbox-Problematik](#)“). Die Diskussion, wie diese technischen Probleme mit den hohen Anforderungen eines rechtsstaatlichen Strafverfahrens an Transparenz, Verfahrensfairness und Menschenrechtsschutz in Einklang gebracht werden können, sollte angesichts der schnellen technischen Entwicklung besser früher als später geführt werden.

