Faire globale Daten-Governance im Sicherheitsbereich? Risiken bei der internationalen Zusammenarbeit von Sicherheitsbehörden und eine mögliche Rolle der Europäischen Union[1]

Hartmut Aden, Sabrina Schönrock, Steven Kleemann und Milan Tahraoui

Zusammenfassung

Dieser Beitrag identifiziert bestehende Schutzlücken bei der internationalen Zusammenarbeit von Sicherheitsbehörden (Polizeibehörden und Nachrichtendienste) und Risiken für die Menschenrechte, die durch Überwachungstechnologien und durch KI-basierte Technologien für die Auswertung von *Big Data* entstehen. Er zeigt, dass Prinzipien wie Fairness, Transparenz oder Erklärbarkeit von Entscheidungen, die auf Anwendungen Künstlicher Intelligenz basieren, bislang innerhalb der Europäischen Union nur unzulängliche und jenseits der EU noch deutlich weniger praktische Wirkungen erzeugen. Dies wird u.a. am Beispiel des sogenannten *EncroChat*-Falls gezeigt. Der Verwirklichung rechtsstaatlicher Grundsätze steht dabei auch die ausgeprägte Geheimhaltungskultur entgegen, die für die internationale Zusammenarbeit von Sicherheitsbehörden prägend ist.

1. Einleitung

Spätestens seit den Enthüllungen durch Edward Snowden im Jahr 2013 ist weithin bekannt, dass Sicherheitsbehörden global nicht nur im großen Stil personenbezogene Daten sammeln und auswerten, sondern diese auch intensiv austauschen. Für die Betroffenen ist diese Praxis weitgehend intransparent, auch mit der Folge, dass sie sich kaum dagegen gerichtlich zur Wehr setzen können. Auch Staaten wie die Bundesrepublik Deutschland, die sich

1 Teile dieses Beitrags basieren auf Erkenntnissen aus den Forschungsprojekten *FAKE-ID: Videoanalyse mit Hilfe künstlicher Intelligenz zur Detektion von falschen und manipulierten Identitäten* und *VIKING: Vertrauenswürdige Künstliche Intelligenz für polizeiliche Anwendungen,* beide gefördert vom Bundesministerium für Bildung und Forschung (BMBF), FKZ: 13N15737 (FAKE-ID) bzw. 13N16241 (VIKING).

als ausgeprägte Rechtsstaaten verstehen, beteiligen sich hieran intensiv, aber oftmals in rechtlichen Grauzonen, wie u. a. das Verfahren vor dem Bundesverfassungsgericht zur Überwachung internationaler Telekommunikation durch den Bundesnachrichtendienst (BND) gezeigt hat.[2] Obwohl bereits seit einiger Zeit sichtbar ist, dass hierfür im Interesse des Menschenrechtsschutzes völkerrechtliche Regelungen erforderlich sind, haben diese bislang kaum Fortschritte gemacht. Durch die zunehmende Bedeutung von Methoden Künstlicher Intelligenz (KI) hat sich das Risiko weiter erhöht, dass die massive Datensammlung und der globale Datenaustausch im Sicherheitsbereich zu intensiveren Grundrechtsbeeinträchtigungen führen.

Risiken entstehen im internationalen Kontext u. a. dann, wenn unklar ist, woher die verwendeten Daten stammen und wie zuverlässig sie sind. Das ist auch innerhalb der Europäischen Union (EU) problematisch. Im Rahmen des Prinzips gegenseitiger Anerkennung, das die EU-Innen- und Justizpolitik seit den 1990er Jahren prägt,[3] wird davon ausgegangen, dass es sich um eine rechtmäßige Erhebung handelt, allein weil diese Daten in einem Mitgliedstaat der EU nach den dortigen Regeln erhoben wurden. Auf der Basis dieses Prinzips würden die Daten also ungeprüft übernommen, da eine rechtmäßige Erhebung grundsätzlich unterstellt würde. Auch der Rückgriff des Staates auf private Akteure mit dem Ziel der Datengewinnung kann zu Risiken für die Grundrechte von Betroffenen führen.[4] Hier besteht insbesondere die Gefahr der Umgehung von Anforderungen, an welche staatliche Behörden gebunden sind, da die privaten Unternehmen die Daten möglicherweise auf Wegen erlangt haben, die Sicherheitsbehörden verwehrt sind.

Das EU-Recht stellt zwar in seinem Zuständigkeitsbereich, zu dem der polizeiliche, nicht aber der nachrichtendienstliche Informationsaustausch gehört (Art. 4 Abs. 2 S. 3 AEUV), zunehmend Anforderung an eine Herkunftsdokumentation von übermittelten Daten sowie relativ hohe Anforderungen an die Datenübermittlung in Nicht-EU Länder;[5] Ausnahmeregelungen im Hinblick auf nationale Sicherheitsinteressen gehen dabei allerdings

2 BVerfGE 154, 152.

3 *Aden*, in Lisken/Denninger (Hrsg.), Polizeirecht, 2021, 7. Aufl., Rn. M 73; *Lavenex*, Journal of European Public Policy 2007.

4 Hierzu z. B. *Lowe*, Rutgers Computer & Technology Law Journal 2021, 1 (38-39).

5 Vgl. etwa ECLI:EU:C:2015:650, Schrems-I; im Sekundärrecht z. B. Art. 23 Abs. 8 Europol-VO (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol), zuletzt geändert durch VO (EU) 2022/991.

zulasten des Grundrechtsschutzes. Die *Schrems-I-* und die *Schrems-II*-Entscheidung des Europäischen Gerichtshofs (EuGH)[6] enthalten wichtige Hinweise auf die Rolle des Privatsektors bei der Generierung von *Big Data*.

Die sogenannte *EncroChat*-Affäre zeigt die weitreichenden Auswirkungen, die unklare Datenverantwortlichkeit auf gerichtliche Verfahren haben kann.[7] In dieser Affäre erhielten deutsche Behörden durch den Datenaustausch mit französischen Behörden Zugriff auf Kommunikationsdaten deutscher Staatsangehöriger in Deutschland, wobei fraglich ist, ob diese nach deutschem Recht hätten erhoben werden können und ob diese in einem Strafverfahren verwertet werden dürfen. Hierzu gibt es bisher keine einheitliche Rechtsprechung: So hält das Landgericht Berlin die Nutzung für unzulässig[8] - im Gegensatz z. B. zum Oberlandesgericht Hamburg,[9] das kein Beweisverwertungsgebot angenommen hat. Der Bundesgerichtshof (BGH) hat bereits dem Grunde nach entschieden, dass die Daten aus dem *EncroChat* Messenger auch in deutschen Strafverfahren genutzt werden können.[10] Das Bundesverfassungsgericht (BVerfG) wird hierüber im Rahmen eines anhängigen Verfassungsbeschwerdeverfahrens zu entscheiden haben.[11] Voraussichtlich werden auch der EuGH und der Europäische Gerichtshof für Menschenrechte (EGMR) mit diesem Fall befasst werden.[12] Angesichts ihrer bisherigen Rechtsprechung könnten sie durchaus zu einer anderen Einschätzung als der BGH kommen.[13]

Dieser Beitrag identifiziert bestehende Schutzlücken bei der internationalen Zusammenarbeit von Sicherheitsbehörden und Risiken für die Menschenrechte, die durch KI-basierte Technologien für die Auswertung von *Big Data* entstehen. Rechtsprechung (EuGH, EGMR, nationale Verfassungsgerichte) und Dokumente mit regulatorischen Intentionen werden hinsichtlich ihres Potenzials untersucht, bestehende Lücken bei der rechtsstaatlichen Einhegung der Daten-Governance im Sicherheitsbereich

6 ECLI:EU:C:2020:559, Schrems-II.
7 Siehe dazu z.B. *European Union Agency for Criminal Justice Cooperation*, Pressemitteilung vom 2.7.2020.
8 LG Berlin, Beschluss vom 1.7.2021 (525 KLs) 254 Js 592/20 (10/21).
9 OLG Hamburg, Beschluss vom 29.01.2021 - 1 Ws 2/21.
10 Ausführlich in BGH, Beschluss des 5. Strafsenats vom 2.3.2022 - 5 StR 457/21.
11 Anhängig unter dem Aktenzeichen: 2 BvR 558/22.
12 *Europäisches Parlament*, EncroChat's path to Europe's highest courts, 2022.
13 Siehe beispielsweise ECLI:EU:C:2022:703 zur Vorratsdatenspeicherung oder CE:ECHR:2021:0525JUD005817013 (Big Brother Watch ua/Vereinigtes Königreich) zur Datenerfassung, -verarbeitung und -übermittlung.

zu schließen. Hierzu zählen internationale Anforderungen, welche sich beispielsweise aus dem *Report on the Democratic oversight of Signals Intelligence Agencies*[14] der Venedig-Kommission oder Ausführungen des UN-Menschenrechtsrats[15] ergeben. Der Verwirklichung rechtstaatlicher Grundsätze steht allerdings eine ausgeprägte Geheimhaltungskultur entgegen, die für die internationale Zusammenarbeit von Sicherheitsbehörden prägend ist.[16]

In diesem Kontext ist auch die globale Rolle der EU von Interesse. EU-Regulierungsansätze können weitreichende faktische Auswirkungen weit über die EU hinaus haben, was etwa für Elemente der Datenschutz-Grundverordnung (DSGVO) vielfach gezeigt worden ist.[17] Auch der Entwurf einer EU-Verordnung zur Künstlichen Intelligenz, den die Europäische Kommission im April 2021 vorgelegt hat, lässt Ambitionen für regulatorischen Einfluss über die EU hinaus erkennen.[18] Als im globalen Maßstab wirtschaftlich starker Akteur hat die EU die Möglichkeit, über Zugangsregeln für den EU-Markt weitreichenden Einfluss auf die Regulierungsstrategien anderer Länder und das Verhalten globaler Konzerne zu nehmen. Der Beitrag fragt, inwieweit dieser Effekt auch für die internationale Daten-Governance im Sicherheitsbereich relevant werden kann. Strukturelle Grenzen sind dem allerdings durch die begrenzten Zuständigkeiten der EU im Sicherheitsbereich (insbesondere bzgl. der Nachrichtendienste) und durch gegenläufige Interessen anderer global mächtiger ökonomischer Akteure (USA, China) gesetzt.

2. Risiken für personenbezogene Daten bei der internationalen Zusammenarbeit der Sicherheitsbehörden

Die internationale Informationszusammenarbeit der Sicherheitsbehörden führt zu mehreren Dimensionen von Risiken für personenbezogene Daten und damit für die Privatsphäre der Betroffenen: im Hinblick auf defizitäre Rechtsstaatlichkeit in beteiligten Staaten, international unterschiedliche Grundrechtsstandards bei der Datenverarbeitung und spezielle Risiken bei

14 CDL-AD(2015)011 vom 15.12.2015.
15 A/HRC/48/31 vom 15.09.2021.
16 Näher hierzu *Aden*, WEP 2018, 981.
17 Auch „Brussels Effect" genannt. Siehe dazu *Bradford*, The Brussels Effect, 2020.
18 *Europäische Kommission*, COM(2021) 206 final, 2021/0106(COD), s. dort insbesondere Erwägungsgrund 5.

der Analyse großer Datenmengen (*Big Data*) mithilfe von Anwendungen Künstlicher Intelligenz.

2.1 Risiken aufgrund defizitärer Rechtsstaatlichkeit in beteiligten Staaten

Die Zusammenarbeit mit Sicherheitsbehörden anderer, insbesondere außereuropäischer Staaten, welche geringere Anforderungen an rechtsstaatliches Handeln, vor allem an den Daten- und Grundrechtsschutz sowie an verfahrenssichernde Maßnahmen als das europäische Recht stellen, kann zu weitreichenden Problemen führen. Als Maßstab gelten hier sowohl verfahrensrechtliche Prinzipien im Sinne des *Fair Trial* aus Art. 6 EMRK als auch grundrechtliche Ausprägungen zur Sicherung des Rechts auf Datenschutz und Privatsphäre. Die Datenübermittlung kann dabei ebenso problematisch sein wie die Verwendung und Weitergabe KI-basierter Systeme und Technologien, welche durch Sicherheitsbehörden eingesetzt werden. Die Risiken sind dabei vielfältig und umfassen beispielsweise die Nutzung von Daten, die im Land der Erhebung für die Personen keinerlei Auswirkungen haben, aber durch Weitergabe an Länder mit geringeren Schutzstandards erhebliche negative Folgen haben können, bis hin zu Verfahren, die zur Todesstrafe führen.

Innerhalb der EU ist der Datenaustausch für Strafverfolgungszwecke inzwischen weitreichend durch EU-Recht geregelt, das auf den Prinzipien der Verfügbarkeit und der gegenseitigen Anerkennung basiert: Die EU-Staaten sollen im Interesse effektiver Strafverfolgung bei ihnen verfügbare Daten möglichst miteinander teilen und dabei auf der Basis gegenseitiger Anerkennung handeln.[19] Dem liegt allerdings die nicht ganz unproblematische Hypothese zugrunde, die rechtsstaatlichen Standards seien in allen EU-Staaten gleichermaßen hoch. Zahlreiche EuGH-Entscheidungen, u. a. zur Überstellung aufgrund eines Europäischen Haftbefehls, deuten indes darauf hin, dass hier weiterhin eine differenzierende Bewertung geboten ist.[20] Zum Datenaustausch mit Drittstaaten hat der EuGH ebenfalls Maßstäbe definiert. Demnach muss in einem Drittstaat nicht zwingend ein identisches Schutzniveau wie in der EU bestehen, jedoch muss entweder aufgrund innerstaatlicher Regelungen oder internationaler Verpflichtungen

19 Näher hierzu *Aden,* in Lisken/Denninger (Hrsg.), Polizeirecht, 2021, 7. Aufl., Rn. M 230 ff.; *Lavenex*, Journal of European Public Policy 2007.

20 *Aden,* in Lisken/Denninger (Hrsg.), Polizeirecht, 2021, 7. Aufl., Rn. M ., Rn. 71 ff. m.w.N.

ein tatsächlicher menschenrechtlicher Schutzstandard bestehen, der dem des EU-Rechts und insbesondere der DSGVO gleichwertig ist.[21] Dies wurde in der *Schrems-II*-Entscheidung für die USA erneut verneint.[22] Grund dafür ist beispielsweise die fehlende Unabhängigkeit des nach US-Recht organisierten Ombudsmann-Mechanismus von der Exekutive.[23] Weiterhin sind insbesondere die weitreichenden Überwachungsbefugnisse der US-Behörden und deren rechtliche Grundlagen[24] nicht mit dem europäischen Grundsatz der Verhältnismäßigkeit vereinbar, wie ihn der EuGH versteht.

Bezüglich der Rechtsstaatlichkeit des Auslandsdatentransfers ist es allerdings auch nicht ratsam, den Blick einseitig auf die USA zu lenken und ausschließlich die dortige Überwachungspraxis zu kritisieren. Der aktuelle Angemessenheitsbeschluss zur Datenübermittlung in das Vereinigte Königreich, welches ebenfalls seit Jahrzehnten ein rigoroses Überwachungsregime etablierte und Mitglied der Geheimdienstallianz *Five Eyes* ist und dennoch ein angemessenes Datenschutzniveau besitzen soll, zeigt die etwas inkonsistente Haltung der EU-Kommission in diesem Zusammenhang.[25]

2.2 Risiken aufgrund unterschiedlicher grundrechtlicher Datenverarbeitungs-Standards

Aufgrund unterschiedlicher grundrechtlicher Datenverarbeitungs-Standards besteht das Risiko, dass unrechtmäßig erhobene Daten im internationalen Bereich weiterverarbeitet und sodann sogar zu Beweiszwecken in der Strafverfolgung eingesetzt werden. Am aktuellen Beispiel der sog. *EncroChat*-Verfahren wird dies in besonderer Weise deutlich. Hier gelang es den französischen Ermittlungsbehörden in einer europäisch koordinierten Aktion in Zusammenarbeit mit Behörden aus den Niederlanden, Europol und Eurojust den Kommunikationsdienst *EncroChat* zu infiltrieren.[26] Die französischen Ermittler:innen vermuteten, dieser werde in erheblichem Umfang von Täter:innen aus der organisierten Kriminalität genutzt. Zunächst wurde Schadsoftware (Trojaner) auf die in Frankreich befindlichen Server des Unternehmens eingespielt. Von dort wurden die Endgeräte

21 ECLI:EU:C:2020:559, „Schrems-II", Rn. 94.
22 Ebd., Rn. 168.
23 Ebd., Rn. 190-198.
24 Insbesondere Section 702 des Foreign Intelligence Surveillance Acts (FISA) und Executive Order 12333.
25 *Kipker,* ZD 2021, 397 (398).
26 BGH, Beschluss des 5. Strafsenats vom 2.3.2022 - 5 StR 457/21, Rn. 8.

sämtlicher Nutzer:innen weltweit „infiziert", was das Auslesen der auf den Telefonen gespeicherten Daten und der darüber geführten Kommunikation ermöglichte. Die erlangten Daten wurden sodann den nationalen Strafverfolgungsbehörden über Europol zur weiteren Verwendung zur Kenntnis gegeben. Inwieweit dabei bereits KI-basierte Auswertungsmethoden verwendet wurden, ist nicht bekannt.

Angesichts des Umfangs und der Eingriffstiefe der heimlichen Überwachungsmaßnahme stellt sich nicht nur die Frage nach der Verwertbarkeit der erlangten Beweismittel in einem deutschen Strafverfahren, gemessen an den Voraussetzungen und Begrenzungen des deutschen Strafverfahrensrechts,[27] sondern auch nach dem internationalen Aspekt der (ggfs. rechtswidrigen) Erhebung der Daten durch die französischen Behörden und der Übermittlung an die deutschen Strafverfolgungsbehörden im Rahmen der Rechtshilfe.[28]

Überprüfbarkeit der Datenverarbeitung und Recht auf faires Verfahren

Die Art und Weise, wie die *EncroChat*-Daten erlangt wurden, beschränkt ihre Nachprüfbarkeit. Der Verfassungsgerichthof Frankreichs (*Conseil Constitutionnel*) bestätigte in einer Entscheidung vom 8. April 2022 zwar, dass die Geheimhaltung der technischen Vorgänge um die Erlangung der *EncroChat*-Daten in Frankreich als ein nationales Militärgeheimnis (*secret défense*) verfassungsgemäß sei und die Verfahrensrechte Beschuldigter – insbesondere das Recht auf ein faires Verfahren gemäß Art. 6 EMRK – nicht beeinträchtigt seien. Jedoch verwies er zugleich auf die erforderliche strafprozessuale Transparenz hinsichtlich der staatlichen „Hacking-Operation".[29] Das französische Verfassungsgericht äußerte sich dahingehend, dass Techniken und Verfahren nachrichtendienstlicher Informationsgewinnung zu schützen seien. In diesem Zusammenhang betonten die Richter:innen, wie wichtig der vertrauliche Charakter solcher Verfahren sei.[30] Auffällig hierbei ist, dass sich das Gericht dabei auf die nachrichtendienstlichen Anforderungen und Techniken beruft, obwohl es im Fall *EncroChat* um die Rechtmäßigkeit des Handelns der beteiligten Strafverfolgungsbehörden ging. Dass die Maßnahme der französischen Behörden konzeptionell auf

27 Hierzu ausführlich *Derin/Singelnstein*, NStZ 2021, 449; *Ruppert*, NZWiSt 2022, 221 (224f.).
28 Zu den Grundlagen der Rechtshilfe: *Pauli*, NStZ 2021, 146 (147f.).
29 Conseil Constitutionnel, Décision n° 2022-987 QPC vom 8.4.2022, 6, Rn. 8.
30 Ebd., S. 7, Rn. 15.

die Erfassung einer großen Anzahl Nichtverdächtiger angelegt war und die eingriffsintensive Maßnahme nicht auf einem individualisierten Tatverdacht beruhte, ist nicht nur nach dem deutschen Recht rechtswidrig,[31] sondern auch nach internationalen rechtsstaatlichen Maßstäben mehr als problematisch. Bemerkenswerterweise entschied das französische Verfassungsgericht, dass die Vorschriften der französischen Strafprozessordnung (Artikel 230-1 bis 230-5 und 706-102-1 *Code de procédure pénale*), deren Verfassungsmäßigkeit in diesem Fall strittig war, tatsächlich ein angemessenes Gleichgewicht (im Original „*une conciliation équilibrée*") zwischen mehreren, aus der französischen Verfassung abgeleiteten Anforderungen herstellen.

Dabei stützte sich die Entscheidung auf drei Kernargumente:[32] Erstens habe das Ziel des französischen Gesetzgebers bei der Verabschiedung der angefochtenen strafprozessualen Maßnahmen darin bestanden, den Ermittlungsbehörden effiziente Mittel zur Sammlung und Entschlüsselung von Daten zur Verfügung zu stellen, ohne den vertraulichen Charakter der von den Nachrichtendiensten zu diesem Zweck eingesetzten Techniken zu schwächen. Diese gesetzgeberischen Maßnahmen trügen daher, so der Gerichtshof, zu den „Zielen des Verfassungswertes" der Suche nach den Urhebern von Straftaten bei und dienten den verfassungsrechtlichen Anforderungen in Bezug auf „die grundlegenden Interessen der Nation".[33] Zweitens stellten die französischen Verfassungsrichter:innen in ihrer Argumentation darauf ab, dass die Durchführung besonderer Ermittlungsmaßnahmen von Richter:innen genehmigt und durch die Notwendigkeit einer Untersuchung im Zusammenhang mit besonders komplexen und schweren Straftaten gerechtfertigt werden muss. Dieses Verfahrenserfordernis stelle daher für das französische Verfassungsgericht implizit eine Garantie für den Schutz der Interessen der Rechtstaatlichkeit und der Grundrechte dar.[34] Drittens nahmen die französischen Verfassungsrichter:innen zur Kenntnis, dass die angefochtenen gesetzgeberischen Maßnahmen es den Ermittlungsbehörden zwar ermöglichen, einige technische Informationen aufgrund des Militärgeheimnisses als streng geheime Verschlusssache zu schützen und so aus dem Geltungsbereich des strafprozessualen Grundsatzes der „Waffengleichheit"

31 BVerfG, Urteil vom 16.2.2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 32, 134; *Arzt*, in: Lisken/Denninger (Hrsg), Handbuch des Polizeirechts, 2021, 7. Aufl., Rn. G 1184 ff.
32 Conseil Constitutionnel, Décision n° 2022-987 QPC vom 8.4.2022, S. 8, Rn. 19.
33 Ebd., S. 7, Rn. 15.
34 Ebd., S. 7, Rn. 16.

herauszunehmen. Sie vertraten jedoch die Auffassung, diese gesetzlichen Regelungen seien in Ordnung, da andere Informationen nach wie vor der Dokumentationspflicht durch die genehmigenden Richter:innen unterlägen. Im Falle der Nichteinhaltung könnten die Maßnahmen darüber hinaus für nichtig erklärt werden. Außerdem verweist das Gericht auf die gesetzliche Vorschrift, dass alle Informationen, die durch besondere Ermittlungsmaßnahmen zum Aufbrechen verschlüsselter Kommunikation gewonnen und an die Ermittlungsbehörden übermittelt werden, zwingend mit der Vorlage einer Bescheinigung einhergehen müssen. Mit dieser Bescheinigung gewährleistet die Organisation, die diese Techniken einsetzt, die „Aufrichtigkeit" der Ergebnisse der besonderen Ermittlungsmaßnahmen.[35]

Die geforderte „Aufrichtigkeitsbescheinigung" von „technischen Organisationen", d. h. möglicherweise auch von Privatfirmen, die auf sicherheitstechnische Produkte spezialisiert sind, wurde in der französischen Rechtsdiskussion als reine Formalität angesehen,[36] bei der eine mögliche Nichteinhaltung von den Strafverfolgungsbehörden einfach korrigiert werden kann. Dies zeigt, dass das französische Recht bei der Regulierung spezieller Ermittlungstechniken, die von Strafverfolgungsbehörden eingesetzt werden, besonders permissiv ist, insbesondere im Vergleich zum deutschen sowie internationalen und europäischen Recht. Angesichts dieser Unterschiede erscheint die Entscheidung des Bundesgerichtshofs, nach der *EncroChat*-Daten keinem Verwertungsverbot unterliegen sollen,[37] kritikwürdig.

Auswirkungen in Großbritannien

In einem *EncroChat*-Verfahren am Londoner *Central Criminal Court* kamen IT-Forensiker vor dem Hintergrund einer Analyse des in Frankreich verwendeten „Staatstrojaners" zu dem Ergebnis, dass dessen Zuverlässigkeit durchaus zweifelhaft sei.[38] Ohne Rückverfolgbarkeit der Daten im Verarbeitungsprozess könne nicht eindeutig gesagt werden, ob die verwendeten Daten authentisch seien – es sei denn, weitere unabhängige Beweise bestätigten den Inhalt der Daten. Zudem sei diese Methode der Datenerhebung

35 Ebd., S. 7, Rn. 17.
36 *Pidoux*, Dalloz actualité v. 14. November 2022.
37 BGH, Beschluss des 5. Strafsenats vom 2.3.2022 - 5 StR 457/21, Rn. 32 ff.
38 *Campbell,* The Guardian v. 14. März 2022.

nicht mit den in Großbritannien geltenden Regeln und Prinzipien zum forensischen Umgang mit digitalen Beweisen vereinbar.[39]

Das Recht auf ein faires Verfahren (Art. 6 EMRK) stellt Anforderungen auch an die Digitalforensik.[40] Mit den Techniken digitaler Beweiserhebung geht geradezu zwangsläufig die Gefahr einer Verletzung von Art. 6 Abs. 1 EMRK einher.[41] *Big-Data*-Analyse und KI-Anwendungen greifen dabei tief in die herkömmliche Art individueller strafrechtlicher Verantwortung ein und haben massive Auswirkungen auf das individuelle Recht auf ein faires Verfahren und auf „Waffengleichheit". Einerseits besteht eine starke Wissens-Asymmetrie zwischen Angeklagten oder Betroffenen und der Anklage,[42] andererseits werden Transparenz und Erklärbarkeit oftmals unzureichend gewährleistet. Hier könnte, jedenfalls im Rahmen eines Gerichtsprozesses, beispielsweise durch die Offenlegung des Softwarequellcodes „Waffengleichheit" geschaffen werden. Letztlich kann damit jedoch auch noch nicht ausreichend nachvollzogen werden, wie die digitalen Beweise zustande gekommen sind und wie zuverlässig sie sind. Hier geht es um das Zusammenspiel und die Abhängigkeiten zwischen Fairness, Transparenz und Erklärbarkeit von KI-Systemen und der Massendatenverarbeitung (näher hierzu unten, 3.1).

Transparenz der Datenerhebung und -verarbeitung im deutschen Strafverfahrensrecht

Die Frage der notwendigen Überprüfbarkeit der *EncroChat*-Daten, ihrer Authentizität und Integrität wird auch anlässlich der aktuellen Verfahren in Deutschland aufgeworfen. Sind Daten im Ausland nicht nach nationalem Recht rechtmäßig erhoben worden oder kann die Frage der rechtmäßigen Erhebung im nationalen Strafverfahren nicht festgestellt werden, steht die Einhaltung rechtsstaatlicher Verfahrensprinzipien, insbesondere die Gewährleistung von Transparenz und Nachvollziehbarkeit der durch

39 *Goodwin,* Computer Weekly v. 11. März 2022.

40 Siehe zu digitalforensischen Standards beispielsweise: *NIST*, Digital and Multimedia Evidence v. 22. November 2022; *European Network of Forensic Science Institutes*, Best Practice Manual for Digital Image Authentication; *Kävrestad*, Fundamentals of Digital Forensics, 2020.

41 *Ewald*, in: Strafverteidigervereinigungen, Organisationsbüro (Hrsg.), 2018, 268 (270).

42 *Wexler*, UCLA Law Review 2021, 212 (242ff.); *Stoykova*, Computer Law & Security Review, 2021, 1; *Ewald*, in: Strafverteidigervereinigungen, Organisationsbüro (Hrsg.), 2018, S. 268.

polizeiliche Ermittlungstätigkeit erzeugten Beweise, auf dem Spiel. Diese würde ersetzt durch die Akzeptanz eines „Blackbox-Prinzips", in dem die Strafgerichte digitale Beweise als Verurteilungsgrundlage akzeptieren, ohne dass die Möglichkeit ihrer Überprüfung besteht. Das Landgericht Berlin[43] bejahte entgegen den Ansichten der Oberlandesgerichte Bremen, Hamburg, Schleswig und Brandenburg sowie des BGH[44] einen Verstoß gegen EU-rechtliche Vorschriften für die Zusammenarbeit in Strafsachen, da keine Unterrichtung der deutschen Behörden über die Kommunikationsüberwachung einer Person in Deutschland stattgefunden habe und diese auch nicht entbehrlich gewesen sei. Zudem sei die Überwachung durch französische Behörden ein nicht gerechtfertigter Eingriff in das Telekommunikationsgrundrecht gemäß Art. 10 GG und das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG; die Bereitstellung der Daten für die Verwendung durch deutsche Behörden sei ein weiterer eigenständiger und nicht gerechtfertigter Eingriff.

Die 25. Große Strafkammer des Landgerichts Berlin setzte die Hauptverhandlung in einem *EncroChat*-Verfahren aus und legte dem EuGH Fragen zur Zulässigkeit der Datenerhebung und Verwertung von *EncroChat*-Daten zur Vorabentscheidung vor.[45] In dem Vorlagebeschluss stellt das Landgericht 14 Fragen zur Auslegung der Richtlinie (EU) 2014/41 zur Europäischen Ermittlungsanordnung (EEA); dabei geht es unter anderem um die Frage, ob ein deutsches Gericht die EEA für Eingriffsmaßnahmen gegen deutsche Staatsbürger:innen hätte anordnen müssen, wie es sich rechtlich auswirkt, wenn sich eine EEA auf sämtliche auf dem Hoheitsgebiet befindlichen Anschlüsse eines Dienstes erstreckt, obwohl keine konkreten Anhaltspunkte für das Begehen schwerer Straftaten durch individu-

43 LG Berlin,Beschluss vom 1.7.2021 (525 KLs) 254 Js 592/20 (10/21); aufgehoben durch Beschluss des KG Berlin vom 30.8.2021 - 2 Ws 79/21 und zur Eröffnung eines Hauptverfahrens an eine andere Strafkammer verwiesen. Das Gericht stellte fest, die Daten seien nach französischem Recht rechtmäßig erhoben worden und dürften deshalb in Deutschland verwendet und verwertet werden. Dadurch, dass die Erkenntnisse spontan übermittelt wurden und dem § 100b StPO entsprachen, liege kein Verstoß gegen Art. 31 Abs. 1 lit. b) RL-EEA vor. Deutschland habe die Daten zudem verwendet und somit konkludent die Übermittlung genehmigt; so dann auch BGH, Beschluss des 5. Strafsenats vom 2.3.2022 - 5 StR 457/21, Rn. 21 ff.

44 OLG Bremen, Beschluss vom 18.12.2020 - 1 Ws 166/20, Rn. 23, 27, 29; OLG Schleswig, Beschluss vom 29.4.2021 - 2 Ws 47/21, Rn. 22; OLG Brandenburg, Beschluss vom 9.8.2021 - 2 Ws 113/21, Rn. 14; BGH Beschluss vom 2.3.2022 – 5 StR 457/21.

45 LG Berlin, Beschluss vom 19.10.2022 - (525 KLs) 279 Js 30/22 (8/22).

elle Nutzer:innen bestehen, ob Daten von Frankreich nach Deutschland übermittelt werden dürfen, auch wenn die Datenerhebung in Deutschland unzulässig wäre oder ob sich durch eine unionsrechtswidrige Ermittlungsanordnung ein Beweisverwertungsverbot ergibt. Die Entscheidung des EuGHs zu den aufgeworfenen rechtlichen Unklarheiten steht noch aus.

Perpetuierter Rechtsverstoß bei grenzüberschreitendem Datentransfer

Im Zusammenhang mit dem hier untersuchten *EncroChat*-Fall geht es im Kern nicht um die Rechtmäßigkeit der Maßnahme nach französischem Recht, sondern um die Frage, ob und unter welchen Voraussetzungen die im Ausland erhobenen Daten in einem deutschen Strafverfahren verwendet werden können. Der Grundrechtseingriff ist als gravierender einzustufen, wenn die Daten nicht nur nach deutschem Recht nicht hätten erhoben werden dürfen (sog. hypothetischer Ersatzeingriff), sondern (nach diesem Maßstab hypothetisch) rechtswidrig erhobene Daten gleichsam „wider besseren Wissens" zu einem abweichenden Maßstab bei der Verwendung im Strafverfahren durch die deutschen Behörden führt. Die in Frankreich und zum Teil von den französischen Behörden auch in Deutschland erhobenen Daten wurden von den Endgeräten erhoben, gespeichert, zusammengeführt, versandt und aufbereitet – also mehrfach verarbeitet. Die Integrität mehrfach verarbeiteter Daten ist gefährdet, wenn die Erhebung und Verarbeitung nicht durch die Einhaltung einheitlicher (europa-)rechtlicher Vorgaben sowie technisch-organisatorischer Maßnahmen sichergestellt wird.[46] Sollen die „abgeschöpften" Daten im deutschen Strafprozess zum Beweis geeignet sein, ist Voraussetzung für eine nachvollziehbare Datenauthentizität und -integrität eine rechtlich wie auch technisch transparente Erhebung der Daten im Ausland. Die Vearbeitung muss in einer „Legitimationskette" (englisch: „chain of custody") bis zur Einbringung in das Gerichtsverfahren nachvollziehbar sein.

2.3 Risiken der KI-basierenden Big Data-Analyse

Die beschriebenen Problematiken des *EncroChat*-Falls stehen exemplarisch für die Schwierigkeiten der *Big-Data*-Nutzung durch Sicherheitsbehörden. Basiert die internationale Zusammenarbeit der Sicherheitsbehörden auf

46 So auch: *Kipker/Bruns*, MMR 2022, 363 (365f.).

KI-Anwendungen, was im *EncroChat*-Fall nicht öffentlich bekannt ist, so vergrößern sich die Risiken für die Grundrechte der Betroffenen erheblich.

Die Risiken einer KI-basierten Datenanalyse durch polizeilich genutzte Technologien sind vielfältig. Dazu zählen die oftmals fehlende oder unklare Rechtsgrundlage für den Verarbeitungszweck, Diskriminierungs- und Biasrisiken ebenso wie weitreichende Eingriffe in das Recht auf informationelle Selbstbestimmung, das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (beide geschützt durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und das Telekommunikationsgrundrecht (Art. 10 GG). Ähnliche Risiken für diese Rechtsgüter bestehen auch auf internationaler Ebene.[47] Mit Blick auf den technischen Fortschritt sowie auf das Tempo der KI-Entwicklung und *Big-Data*-Analysen muss davon ausgegangen werden, dass sich die Risiken erhöhen werden.

Diskriminierungsrisiken bestehen hier beispielsweise aufgrund von Geschlecht, ethnischer Herkunft, Behinderungen, Religion und Glaube, Alter oder sexueller Orientierung. Durch *Big-Data*-Analysen können bereits bestehende Diskriminierungsdynamiken und -gefahren um ein Vielfaches erhöht und automatisiert reproduziert und verfestigt werden. Generell entstehen mit Blick auf KI-basierte Systeme *Bias*-Risiken bereits und zuvörderst im Zusammenhang mit den Trainingsdatensätzen. Sind diese Risiken bereits in den Trainingsdaten angelegt, werden diese durch das Trainieren des KI-basierten Systems fortgeführt und möglicherweise noch verstärkt. Demzufolge müssen im Zusammenhang mit polizeilichen Grundrechtseingriffen hier besonders hohe Anforderungen gestellt und erfüllt werden.

Mit der Überarbeitung der Europol-Verordnung, welche seit dem 28. Juni 2022 gilt,[48] haben sich einige Neuerungen für die internationale Datenverarbeitung ergeben. Auf europäischer Ebene ist die EU-Agentur für die Zusammenarbeit im Bereich Strafverfolgung (Europol) ein zentraler Akteur; insbesondere bezüglich Datenverarbeitung und Datenaustausch kommt Europol eine wesentliche Rolle zu. Die Verarbeitung und Analyse von Daten ist bereits primärrechtlich in Art. 88 Abs. 2 S. 2 lit. a AEUV als Aufgabe von Europol angelegt. Allerdings sah der Europäische Datenschutzbeauftragte (EDSB) unter der bisherigen Europol-Verordnung,[49] anders als die Europol-Agentur selbst, das tatsächliche Vorgehen von Europol

47 *OHCHR*, The right to privacy in the digital age, Report of the United Nations High Commissioner for Human Rights, A/HRC/39/29 vom 3.8.2018.

48 VO (EU) 2022/991.

49 VO (EU) 2016/794.

teilweise als nicht vom geltenden Recht gedeckt an. Der EDSB rügte die Verarbeitung von *Big-Data* zu Analysezwecken als rechtswidrig und verpflichtete Europol im Januar 2022, die betroffenen Datensätze zu löschen.[50] Als direkte Reaktion darauf wurde in der Neufassung der Europol-Verordnung ein neuer Art. 18 Absatz 6a eingefügt. Damit soll klargestellt werden, dass die Agentur eingehende Daten vorab analysieren und feststellen kann, ob diese unter eine der zulässigen Kategorien des Art. 18 Europol-VO fallen. Die betreffenden Daten sollen dann auch mit bereits vorliegenden abgeglichen werden dürfen.[51] Dadurch kann Europol grenzüberschreitende Querverbindungen erfassen, welche die nationalen Behörden so nicht selbst hätten feststellen können. Problematisch ist hierbei, dass Europol nicht nur Daten über verurteilte Straftäter:innen und Tatverdächtige verarbeiten darf, sondern auch über „Personen, in deren Fall nach Maßgabe des nationalen Rechts des betreffenden Mitgliedstaats faktische Anhaltspunkte oder triftige Gründe dafür vorliegen, dass sie Straftaten begehen werden, für die Europol zuständig ist."[52] Eine solch weitgehende und unbestimmte Formulierung erfasst potenziell auch Verhaltensweisen, welche weit im Vorfeld eventueller Straftaten liegen und genügt damit nur schwerlich den Anforderungen an die Bestimmtheit einer Eingriffsnorm.[53]

Ebenfalls in diesem Zusammenhang kann auf den neuen Art. 18a Europol-VO verwiesen werden, wonach nationale Strafverfolgungsbehörden nunmehr Europol mit der Auswertung von Daten beauftragen können, sofern diese auch unter dem entsprechenden nationalen Rechtsrahmen in Ermittlungsverfahren ausgewertet und erhoben werden dürfen.[54] Damit wurde auf Bedenken des EDSB eingegangen und der Versuch unternommen, rechtlich klarzustellen, dass die Datenverarbeitung und Datenübermittlung möglich sind, solange sie den rechtlichen Anforderungen im jeweiligen Mitgliedsstaat genügen.

Auch die Neuregelungen der Europol-VO zum Informationsaustausch mit Drittstaaten (Art. 25 Europol-VO) und der Abschnitt zur Zusammenarbeit mit Privaten (Art. 26 ff. Europol-VO) sind im Hinblick auf eine faire Daten-Governance problematisch. Der neue Art. 25 Abs. 4a Europol-VO er-

50 EDSB, Entscheidung vom 17.9.2020 – C 2019-0370, S. 7 f.; EDSB, Entscheidung vom 21.12.2021 – C 2021-0699.
51 *Rüß/Lutz*, GSZ 2022, 221 (223).
52 Europol-VO Anhang II, Abschnitt A, Abs. 1 lit. b.
53 *Aden*, in Lisken/Denninger (Hrsg.), Polizeirecht, 2021, 7. Aufl., Rn. M 214.
54 *Rüß/Lutz*, GSZ 2022, 221 (223).

weitert Europols Möglichkeiten zum strukturellen Datenaustausch, ähnlich jenen von Eurojust, und ermöglicht damit Ausnahmen oder gar die Umgehung eines Angemessenheitsbeschlusses der EU-Kommission oder des Erfordernisses eines bestehenden Abkommens nach Art. 218 AEUV. Damit kann Europol künftig auch personenbezogene Daten übermitteln, wenn geeignete Datenschutzgarantien in einem rechtsverbindlichen Instrument vorgesehen sind oder die Agentur selbst alle Umstände der Datenübermittlung prüft und der Auffassung ist, dass geeignete Garantien für den Schutz von Daten existieren.[55] Eine solche selbstständige Beurteilung ermöglicht zwar eine gewisse Flexibilität bezüglich der besonderen Bedeutung des Informationsaustausches für die innere Sicherheit, beinhaltet aber insbesondere auch mit Blick auf die Rüge des EDSB erhebliche Gefahren für den Grundrechtsschutz.

Auch die Neuregelungen zur Zusammenarbeit von Strafverfolgungsbehörden und Privaten sollten einer kritischen Prüfung unterzogen werden. Der neue Art. 26 Abs. 2 und 4 präzisiert das Verfahren zur Feststellung und Information betroffener Stellen, wenn die Agentur personenbezogene Daten direkt von Privaten entgegennimmt. Europol darf alle betroffenen Stellen ermitteln und die Daten zu diesem Zweck nach Art. 18 Europol-VO verarbeiten und muss diese Daten sowie die relevanten Ergebnisse aus deren Verarbeitung, die für die Feststellung der Zuständigkeit erforderlich sind, unverzüglich an die betreffenden nationalen Stellen weiterleiten. Demgegenüber soll die Weiterleitung an Drittstaaten und internationale Organisationen nun in einer Art pflichtgemäßem Ermessen von Europol liegen.[56] Sofern die private Partei in einem Drittstaat niedergelassen ist, mit dem keine Möglichkeit zum strukturellen Informationsaustausch nach Art. 25 Abs. 1 und 4a Europol-VO besteht, räumt Art. 26 Abs. 4 UAbs. 2 der Agentur schließlich die Möglichkeit ein, diesem das Ergebnis der Verarbeitung unter den Voraussetzungen von Art. 25 Abs. 5 und 6 weiterzuleiten. Der neue Art. 26 Abs. 5 Europol-VO behält zwar das Grundprinzip bei, dass die Agentur keine personenbezogenen Daten an private Akteure übermitteln darf, der Katalog der Ausnahmen wurde jedoch erweitert.

Die Neuerungen erweitern somit die Datenverarbeitungsmöglichkeiten und bereiten den Weg für die Agentur zur Verarbeitung großer und komplexer Datensätze.[57] Europol erhält damit ein weitergehendes Mandat als

55 Ebd, 224.
56 Ebd.
57 *Quintel*, EDPL 2022, 90 (92).

bisher, mit privaten Stellen und Drittländern zusammenzuarbeiten. Im Hinblick auf eine wirksame Datenschutzaufsicht für die internationale Daten-Governance der Sicherheitsbehörden erscheint es äußerst problematisch, dass Europol rechtswidrig verarbeitete Daten aufgrund der Rüge des EDSB nicht etwa löschte, sondern die rechtswidrigen Praktiken im Nachhinein durch eine Verordnungsänderung „legalisiert" wurden.

3. Anforderungen an eine faire Daten Governance von Sicherheitsbehörden

In den folgenden Abschnitten werden Anforderungen an eine faire Daten-Governance durch Sicherheitsbehörden skizziert. Dabei ist vorab zu bemerken, dass diese Anforderungen bislang nur fragmentarisch sind und ein ganzheitlicher Blick auf die transnationale Polizeiarbeit und damit einhergehende Menschenrechtsrisiken fehlt. Die voranschreitende Technisierung der Polizeiarbeit erschwert zudem eine wirksame Kontrolle. Dies gilt umso mehr für KI-basierte Polizeiarbeit, bei der die praktische Umsetzung zentraler Prinzipien wie Fairness, Transparenz und Erklärbarkeit von Entscheidungen, die mittels KI-basierter Systeme getroffen werden, sich als große Herausforderung erweist.[58]

3.1 Fairness als Prinzip der Datenverarbeitung

Im Zusammenhang mit der Datenverarbeitung durch Sicherheitsbehörden wird *Fairness* manchmal als erfüllt angesehen, wenn Transparenz gewährleistet ist. Diese Perspektive erscheint jedoch unterkomplex. Transparenz als Anforderung von Datenverarbeitung stellt zwar einen wichtigen Teilaspekt dar, jedoch geht *Fairness* als übergreifendes Konzept darüber hinaus und muss im Zusammenhang mit Erklärbarkeit und Transparenz gesehen werden. Erst durch die Gewährleistung all dieser Prinzipien kann auch ein höheres Maß an Verfahrensgerechtigkeit entstehen. Der internationale Datenaustausch kann die Umsetzung dieser Prinzipien erschweren. Auch die bereits beschriebenen *EncroChat*-Daten und deren Nutzung müssen sich an diesen Prinzipien messen lassen, und insbesondere das Recht auf ein faires Verfahren darf hier nicht umgangen werden.

58 *Aden u.a.*, zfmr 2022, 50 (68f.).

Bezüglich künftiger Regelungen kann auf die geplante EU-Verordnung zu Künstlicher Intelligenz geschaut werden. Es ist in diesem Zusammenhang bemerkenswert, dass der Begriff *Fairness* so konkret gar nicht im Verordnungsentwurf vorkommt. Der Fairness-Grundsatz wird jedoch in mehreren europäischen und internationalen Empfehlungen und Regelungen zu KI-Systemen erwähnt.[59] In diesem Kontext steht Fairness in engem Zusammenhang mit dem ethischen und normativen Grundsatz der Nichtdiskriminierung. Darüber hinaus umfasst er auch den rechtlich weniger normierten Aspekt, dass KI-basierte Entscheidungen so ausgestaltet sein sollen, dass Betroffene das Ergebnis als fair und akzeptabel wahrnehmen können – ein Aspekt, der auch in *Procedural Justice*-Theorien zur Akzeptanz von Behördenhandeln eine zentrale Rolle spielt.[60] Damit ist Fairness sowohl als rechtliche als auch ethische Kategorie anzusehen und kann zusätzlich aus unterschiedlichen, auch technischen, Blickwinkeln betrachtet werden. Algorithmische Fairness meint beispielsweise solche Methoden, die Verzerrungen in datenverarbeitenden Systemen verringern oder ausschließen, wenn diese zu sozialen Stigmatisierungen oder Diskriminierungen führen können. In der Informatik wird dabei auch zwischen individueller und gruppenbezogener Fairness unterschieden.[61] Bei Gruppenfairness sollen die Ergebnisse beispielsweise eines KI-Systems so angeglichen werden, dass für unterschiedliche vordefinierte Gruppen diese gleich oder zumindest ähnlich sind; individuelle Fairness soll sicherstellen, dass die Ergebnisse für vergleichbare Individuen auch gleich sind.[62] Für den Kontext der Sicherheitsbehörden und deren Datenverarbeitung und -austausch folgt daraus, dass die effektive Gewährleistung von Fairness, aber auch von Transparenz und Erklärbarkeit, eine besondere Herausforderung darstellt. Um dieser zu begegnen und damit insbesondere auch Verfahrensgerechtigkeit herzustellen, wären adressat:innenspezifische Lösungen ein geeignetes Mittel. Das bedeutet, dass die unterschiedlichen Bedürfnisse an eine faire globale Daten-Governance, an Datenverarbeitung, Datenaustausch und

59 UNESCO Recommendation on the ethics of artificial intelligence, SHS/BIO/REC-AIETHICS/2021; OECD, Empfehlung des Rats zu künstlicher Intelligenz, OECD/LEGAL/0449, 22.5.2019; Europarat, CAHAI, Feasibility Study, CAHAI(2020)23, 17.12.2020; United Nations System CEB/2022/2/Add.1, Chief Executives Board for Coordination Distr.: General 27.10.2022.

60 Näher hierzu *Sunshine/Tyler*, Law and Society Review 2003, 513; *O'Brien/Tyler*, Behavioral Science & Policy 2019, 35.

61 *Mehrabi et al.*, ACM Computing Surveys 2021, 1 (11ff.)

62 Ebd.

eine faire Ausgestaltung KI-basierter Technologien im Rahmen der Arbeit von Sicherheitsbehörden, akteursspezifischen Anforderungen unterliegen. Interessant ist, dass der Verordnungsentwurf auch die Tatsache berücksichtigt, dass die Verarbeitung nicht personenbezogener Daten ebenfalls zu grundrechtlichen Risiken führen kann, weswegen eine solche Datenverarbeitung auch verfahrensrechtlich einzuhegen sei.[63]

Bezüglich dieser Anforderungen kann hier erneut der *EncroChat*-Fall beispielhaft herangezogen werden. Es kann auch in diesem Fall davon ausgegangen werden, dass Ermittler:innen, Gerichtssachverständige, Anwäl:innen, Richter:innen, KI-Fachleute, Beschuldigte, sonst Betroffene und die breite, auch internationale Öffentlichkeit unterschiedliche Bedürfnisse und Interessen bezüglich Fairness, Transparenz und Erklärbarkeit haben. Um dies zu verdeutlichen, könnte nun anhand einer Art „Zwiebelmodell" eine gruppenspezifische Gewährleistung und Offenlegung verschiedener Informationen möglich gemacht werden. Praktisch bedeutet dies, dass im Falle von KI-Anwendungen Fachleuten, denen der Betrieb der KI-Anwendung obliegt, ebenso wie den Ermittelnden und Gerichtssachverständigen, in einer inneren Schicht umfangreiche technische und inhaltliche Informationen zur Verfügung gestellt werden, um KI-basierte Entscheidungen fundiert und kritisch bewerten zu können. Betroffene von KI-basierten Entscheidungen erhalten nach diesem Modell die für sie relevanten Informationen, um eine effektive Grundrechtsausübung gewährleisten zu können, ohne dass diese eine vertiefte technische Expertise benötigen. Die äußere Schicht hält alle für die allgemeine Öffentlichkeit notwendigen Informationen bereit. Um dies zu gewährleisten, müssen differenzierte Anforderungen bereits bei der KI-Entwicklung mitbedacht und von Beginn an in ein holistisches Konzept integriert werden. Wichtige Kriterien sind dabei auch die Partizipationsoffenheit und eine interdisziplinäre, integrierte Technikentwicklung.[64] Die Gesetzgebung wird die Verwirklichung eines solchen Modells durch die Etablierung entsprechender Pflichten für Sicherheitsbehörden gewährleisten müssen. Das Modell könnte den Anforderungen an Fairness im Zusammenhang mit Datenverarbeitung, insbesondere *Big-Data* und deren transnationale Dimension, erfüllen helfen. Im internationalen Kontext wären neben verbindlichem EU-Recht insbesondere

63 *Hornung*, AöR 2022, 147, 1 (66).
64 *Gressel/Orlowski*, TATuP 2019, 71.

völkerrechtliche Standards hierfür hilfreich – die allerdings bisher nicht konkret absehbar sind.[65]

Hieran anschließend stellt sich die Frage, inwieweit die Pflicht zur Wahrung nationaler Grundrechte bei der transnationalen Datenverarbeitung besteht, beziehungsweise inwiefern deutsche Sicherheitsbehörden überhaupt im Rahmen von internationaler Datenverarbeitung an das Grundgesetz gebunden sind. Dies wird nachfolgend erläutert.

3.2 Grundrechtsbindung der Sicherheitsbehörden bei transnationaler Datenverarbeitung

Inwiefern Sicherheitsbehörden im Rahmen von Datenverarbeitung auf trans- und internationaler Ebene an die deutsche Verfassung gebunden sind beziehungsweise wie weit die territoriale Geltung der Grundrechte reicht, war bereits Gegenstand etlicher, auch höchstrichterlicher Entscheidungen. Bereits 1999 hat das BVerfG Aussagen zur Vereinbarkeit strategischer Überwachung der Telekommunikationsbeziehung zwischen Deutschland und dem Ausland durch den BND nach § 3 G 10 a. F. (jetzt § 5 G 10) und zur Reichweite von Art. 10 GG getroffen, musste die Frage jedoch aufgrund fehlender Entscheidungserheblichkeit nicht beantworten.[66] Spätestens mit den Enthüllungen durch Edward Snowden 2013 rückten die Zusammenarbeit und der Datenaustausch zwischen Nachrichtendiensten, deren Kontrolle sowie die fehlende gesetzliche Befugnis des BND zur strategischen Überwachung von Ausland-Ausland-Telekommunikation erneut in den Mittelpunkt öffentlichen Interesses.[67] Als Konsequenz dieser Entwicklungen wurde 2016 das Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des BND[68] verabschiedet. Gegen dieses Gesetz richtete sich sodann eine erfolgreiche Verfassungsbeschwerde, durch die das BVerfG Maßstäbe bezüglich der internationalen Datenverarbeitung, aber insbesondere auch bezüglich der Auslandsgeltung deutscher Grundrechte gesetzt hat.[69] Das BVerfG stellte in dieser Entscheidung – angesichts der Ausgestaltung des Brief-, Post- und Fernmeldegeheimnisses (Art. 10 GG) als „Jedermann"-Grundrecht wenig

65 Hierzu auch *Aden,* in: Delpeuch/Ross (Hrsg.), Comparing the Democratic Governance of Police Intelligence, 2016, 322; *Aden*, WEP 2018, 981.
66 BVerfGE 100, 313, Rn. 173.
67 *Huber,* NVwZ-Beilage 2020, 3 (3).
68 Gesetz vom 23.12.2016 - BGBl. I 2016, Nr. 67, 30.12.2016, S. 3346.
69 BVerfGE 154, 152-312.

überraschend – eine dezidierte Bindung deutscher Staatsgewalt fest und klärte damit die bis dahin umstrittene Frage der territorialen grundrechtlichen Geltung dieses Grundrechts auch für Ausländer:innen im Ausland gegenüber technischer Überwachung ihrer Kommunikation durch deutsche Nachrichtendienste.[70]

Der strategischen Fernmeldeaufklärung wohnt die Besonderheit inne, weitere, eigenständige Grundrechtseingriffe nach sich zu ziehen. Das ist immer dann der Fall, wenn beispielsweise der BND die aus der Überwachung gewonnenen Erkenntnisse an in- und ausländische Behörden weiterleitet.[71] Hier sah das BVerfG die Notwendigkeit, zwingend rechtsstaatliche Garantien zu gewährleisten.[72] Insbesondere dürfen aufgrund der grenzüberschreitenden Kooperation und Übermittlung von Daten keine grundrechtlichen Garantien umgangen werden.[73] Bereits vor dem Urteil war anerkannt, dass die deutsche Staatsgewalt nicht an Menschenrechtsverletzungen im Ausland beteiligt sein darf, weswegen beispielsweise die Schutzpflicht aus Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG Abschiebungen verbietet, bei denen die Gefahr menschenunwürdiger Behandlung droht.[74] Es ist daher nur konsequent, dass die Verfassungsrichter:innen der Staatsgewalt vorschrieben, im Rahmen einer Rechtsstaatlichkeitsvergewisserung sicherzustellen, dass die aus der Überwachung erlangten Informationen im Empfängerstaat nicht zu Verletzungen des menschenrechtlichen Mindeststandards oder der elementaren Regeln des humanitären Völkerrechts führen.[75] Ähnliche Anforderungen folgen auch aus Rechtsprechung des EGMR zur extraterritorialen Informationsgewinnung durch den US-Auslandsnachrichtendienst *Central Intelligence Agency* (CIA). Der EGMR verurteile bereits 2012 Mazedonien (heute Republik Nordmazedonien) unter dem Gesichtspunkt einer Schutzpflichtverletzung aufgrund der Entführung und Überstellung von Khaled El Masri an die CIA im Rahmen des *extraordinary renditions*-Programms,

70 BVerfGE 154, 152, Rn. 87, 92, 104.
71 *Schmahl*, NJW 2020, 2221 (2224).
72 BVerfGE 154, 152, Rn. 211 ff.
73 BVerfGE 154, 152, Rn. 244.
74 BVerfGE 60, 348; BVerfGE 75, 1 (16f.); BVerfGE 113, 154 (162); BVerfGE 140, 317 (347); BVerfGE 141, 220 (342f.).
75 BVerfGE 154, 152, Rn. 233, 237.

bei dem mutmaßlich Terrorverdächtige zur Informationsgewinnung auf fremdes Staatsgebiet verbracht und gefoltert wurden.[76]

Der EGMR hat sich darüber hinaus bereits mehrfach mit Maßnahmen der Überwachung von Telekommunikation von Individuen und der Problematik von „Massenüberwachung" im Bereich der nachrichtendienstlichen Fernmeldeaufklärung befasst.[77] Hier sind insbesondere die Verfahren *Big Brother Watch v UK*[78] und *Rättvisa v Schweden*[79] zu nennen. In dem grundlegenden Urteil der Großen Kammer in der Rechtssache *Big Brother Watch* gegen das Vereinigte Königreich nahm der EGMR auf einige Schlüsselaspekte der BVerfG-Entscheidung zur Ausland-Ausland-Fernmeldeaufklärung des BND Bezug. Dabei nahmen die Straßburger Richter:innen insbesondere die Tatsache zur Kenntnis, dass nach deutschem Recht die internationale Zusammenarbeit mit ausländischen Nachrichtendiensten nicht dazu genutzt werden darf, geltende innerstaatliche Rechtsgarantien zu umgehen.[80] Der EGMR führte weiter aus, welches Recht anzuwenden sei, wenn ein Vertragsstaat Daten von ausländischen Nachrichtendiensten anfordert. Das Gericht formulierte explizit die Anforderung, es sei zu verhindern, dass die Vertragsstaaten ihre Verpflichtungen aus der EMRK umgehen, insbesondere, wenn nachrichtendienstliche Daten von einer Nichtvertragspartei angefordert werden.[81] Weiter muss es auch klare Regelungen bezüglich des Datenaustausches geben, welche die Bürger:innen in die Lage versetzen zu verstehen, wann und unter welchen Bedingungen ein solcher stattfindet; zudem bedarf es dafür einer expliziten gesetzlichen Grundlage im innerstaatlichen Recht.[82] Die Tatsache, dass die internationale nachrichtendienstliche Zusammenarbeit nicht dazu benutzt werden darf, die Verpflichtungen aus der Konvention zu umgehen, gilt nicht nur für die Datenübermittlung an Drittstaaten: Sie gilt auch unter den Vertragsparteien der EMRK selbst.

Diese Anforderungen wurden zwar im Zusammenhang mit Nachrichtendiensten aufgestellt, jedoch lassen sich hier auch für die Strafverfol-

76 Grundlegend dazu: EGMR NVwZ 2013, 631 Rn. 220 – El-Masri. Zur Folgejudikatur vgl. *Staffler*, EuGRZ 2016, 344 (346ff.); *Schmahl* in Dietrich/Sule (Hrsg.), Intelligence Law and Policies in Europe, 2019, 291 (317f.).
77 *Huber*, NVwZ-Beilage 2021, 3 (3f.).
78 CE:ECHR:2021:0525JUD005817013 (Big Brother Watch ua/Vereinigtes Königreich).
79 CE:ECHR:2021:0525JUD003525208.
80 CE:ECHR:2021:0525JUD005817013, Rn. 251.
81 Ebd., Rn. 251.
82 Ebd., Rn. 497.

gungsbehörden einzuhaltende Standards ableiten. Dies gilt umso mehr, weil Daten, welche Polizeien aus dem Ausland erhalten, originär auch von Nachrichtendiensten stammen können – auch vor dem Hintergrund, dass die Zuständigkeitsabgrenzung zwischen Polizeien und Nachrichtendiensten von Land zu Land variiert. Das Argument, es handele sich wahrscheinlich um Datensätze aus Rechtsstaaten und daher sei eine hiesige Verarbeitung gerechtfertigt, kann vor diesem Hintergrund nicht überzeugen. Dadurch würden die vom Bundesverfassungsgericht aufgestellten Kriterien unterlaufen und auch das informationelle Trennungsprinzip[83] umgangen.

Im Zusammenhang mit der internationalen Datenverarbeitung weist das US-amerikanische Rechtssystem indes noch weitaus größere Defizite auf als das europäische. Hier bestehen auch praktisch relevante Zusammenhänge, denn der Austausch von Daten zwischen europäischen Ländern und den USA hat erhebliche Ausmaße, sowohl im privatwirtschaftlichen Bereich als auch bei den Polizeien und Nachrichtendiensten.[84] In den USA sind die datenschutzrechtlichen Standards deutlich weniger ausgeprägt als in Europa. Hinzu kommt die allgemeine US-amerikanische Sichtweise, dass der Grundrechtsschutz in der Regel lediglich für eigene Staatsangehörige gilt.[85] Dies hat zur Folge, dass es schwer ist, den internationalen Datenaustausch zwischen den Ländern grundrechtsschonend zu regeln. Die Verfahren *Schrems-I* und *Schrems-II* verdeutlichen dies.[86] Der EuGH hat in *Schrems-II* zum Ausdruck gebracht, dass er Zweifel daran hegt, „ob das Recht der Vereinigten Staaten tatsächlich das nach Art. 45 der DSGVO im Licht der durch die Art. 7, 8 und 47 der Charta verbürgten Grundrechte erforderliche Schutzniveau gewährleistet."[87] Der Europäische Datenschutzausschuss (EDSA) hat als Reaktion auf *Schrems-II* für Drittstaatentransfers ein sechsstufiges Prüfprogramm vorgeschlagen,[88] damit die Verantwortlichen prüfen können, „ob nebst den Garantien nach Art. 46

83 Vgl. BVerfGE 133, 277, Rn. 123; BVerfGE 156, 11, Rn. 101, 105.

84 Siehe dazu z.B. *Glouftsios/Leese,* Review of International Studies 2023, 125 (129-131); *Bellanova/de Goede*, Regulation & Governance 2022, 102; *Raposo,* Information & Communications Technology Law 2023, 45; *Bäuerle,* CR 2023, 64; *Iliadis/Acker,* The Information Society 2022, 334; PE 694.678, July 2021; ECLI:EU:C:2020:559, „Schrems-II"; *Bignami*, Boston Legal Law Review 2007, 609(655ff.); *Huber*, NVwZ-Beilage 2021, 3 (6ff.).

85 Europäisches Parlament (2021): *Bignami*, GWU Law School Public Law Research Paper 2015, 9; UN Doc A/69/397, 16, Abs. 42; CCPR/C/USA/CO/4, 9f., Abs. 22.

86 *Dehmel u.a.*, MMR 2023, 17 (17).

87 ECLI:EU:C:2020:559, „Schrems-II", Rn 168.

88 EDSA Empfehlungen 01/2020; sowie EDSA Empfehlungen 02/2020.

DS-GVO – insbesondere nebst Standarddatenschutzklauseln nach Art. 46 Abs. 2 lit. c DS-GVO – zusätzliche Maßnahmen vereinbart werden müssen bzw. ob der Transfer trotz möglicher zusätzlicher Maßnahmen zu unterlassen ist."[89] Mittlerweile ist die EU bemüht, ein neues Datenschutzabkommen mit den USA zu schließen. US-Präsident Joe Biden unterzeichnete dazu im Oktober 2022 eine Verfügung (*Executive Order*), die als Grundlage eines neuen Rechtsrahmens für den Datentransfer zwischen den USA und der EU dienen soll.[90] Daran anschließend hat die EU-Kommission ein Verfahren gem. Art. 45 DSGVO zur Annahme eines Angemessenheitsbeschlusses für einen sicheren Datenverkehr mit den USA eingeleitet.[91] Inwiefern dieser Beschluss gefasst wird, ist aktuell noch unklar. Das Europäische Parlament und der EDSA haben noch Vorbehalte.[92]

3.3 Accountability-Anforderungen

Bezüglich der *Accountability*-Anforderungen stellen sich vielfältige Fragen, die ebenfalls durch den Einsatz KI-basierter Systeme und *Big Data*-Anwendungen verschärft werden. Die höhere Eingriffsintensität folgt aus den gestiegenen technischen Möglichkeiten, die zu einer komplexeren Auswertung, der Neugenerierung von Daten, aber auch Intransparenz von Abläufen für Betroffene solcher Maßnahmen führen.[93] In Demokratien wird die Kontrolle der Staatsgewalt durch Transparenz überhaupt erst ermöglicht. Der Sicherheitsbereich ist in diesem Zusammenhang durch ein gewisses Maß an „notwendiger" Intransparenz gekennzeichnet, um den sensiblen Charakter ihrer Ermittlungsfunktion zu wahren.[94] Aufgrund der „*Blackbox*"-Problematik KI-basierter Technologien und des hohen Maßes an Intransparenz solcher Systeme steigt die Gefahr für Demokratie und Menschenrechte durch den sicherheitsbehördlichen Einsatz solcher Systeme. Im Zusammenhang mit Aktivitäten im Rahmen der internationalen Zusammenarbeit von Sicherheitsbehörden tritt hinzu, dass diese häufig auf informellen Vereinbarungen und Praktiken beruhen, bei denen Staaten nur

89 *Dehmel u.a.*, MMR 2023, 17 (18).
90 *The White House*, Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities Executive Order 14086 vom 7.10.2022.
91 Europäische Kommission, Pressemitteilung vom 13.12.2022.
92 EDSA, Pressemitteilung vom 28.2.2023.
93 So die ständige Rspr. des Bundesverfassungsgerichts, vgl. BVerfGE 115, 320 (Rasterfahndung); BVerfGE 156, 11 (Antiterrordateigesetz).
94 *Aden* u.a., zfmr 2022, 50 (57 ff.).

ungern die für die Identifizierung und Bewertung möglicher Menschenrechtsverletzungen nötigen Informationen offenlegen.[95] Auch nach der Rechtsprechung des EGMR steht es Staaten frei, internationale Kooperationsstrukturen einzurichten, um beispielsweise Datensicherheitsoperationen durchzuführen.[96] Allerdings darf dies (gem. dem sog. *Bosporus-Prinzip*[97]) nur erfolgen, sofern und solange das nach der EMRK geltende Niveau des Menschenrechtsschutzes nicht unterlaufen wird.[98] Im Rahmen informeller internationaler Zusammenarbeit können *Accountability*-Mechanismen auch mit Konzepten wie gemeinsamer oder geteilter Verantwortung umrissen werden. Das bedeutet, dass die kooperierenden Staaten gemeinsam für mögliche Datenschutz- oder Menschenrechtsverstöße verantwortlich sind. Wenn Polizeibehörden und Nachrichtendienste international zusammenarbeiten, eröffnet ihnen dies Möglichkeiten, die weiterhin vorwiegend auf nationaler Ebene verankerten *Accountability*-Mechanismen zu umgehen[99] – der *EncroChat*-Fall zeigt dies eindrücklich. Gemeinsame Verpflichtungen, die zu einer gemeinsamen Verantwortung führen, haben sowohl in der Rechtwissenschaft als auch in den politischen Diskursen an Bedeutung gewonnen, sind aber in der Praxis noch nicht konkretisiert worden.[100]

Auch aus der *Big Brother Watch*-Entscheidung des EGMR lassen sich konkrete Anforderungen an eine faire und unabhängige Kontrolle der internationalen Datenverarbeitung ableiten. So betonte der Gerichtshof, es sei notwendig, dass in jedem Stadium der „Massenüberwachung" eine unabhängige Stelle dieses Vorgehen kontrolliert; zudem müsse die Kontrolle „robust" sein.[101] Dazu zählt auch die Verpflichtung der Nachrichtendienste, detaillierte Aufzeichnungen der „Massenüberwachung" zu Kontrollzwecken vorzuhalten. Weiterhin muss die Notwendigkeit und Verhältnismäßigkeit bezüglich der Anwendung von sog. personenbezogenen „starken Suchbegriffen" im Rahmen einer besonderen und objektiven Prüfung schriftlich begründet und behördenintern genehmigt werden.[102] Außerdem

95 *Ryngaert/van Eijk*, International Data Privacy Law 2019 61 (63).
96 Ebd.
97 ECLI:CE:ECHR:2005:0630JUD004503698, „Bosphorus v. Ireland"; Vgl. dazu: *Gonçalves*, JusGov Research Paper No. 2022-05; siehe auch zur Vergleichbarkeit mit Solange Rspr: *Haratsch,* ZaöRV 2006, 927; *Canor,* ZaöRV 2013, 249.
98 *Ryngaert/van Eijk*, International Data Privacy Law 2019, 61 (63).
99 Hierzu näher *Aden*, WEP 2018, 981 (995f).
100 *Ryngaert/van Eijk*, International Data Privacy Law 2019, 61 (64).
101 CE:ECHR:2021:0525JUD005817013, Rn. 356.
102 *Huber,* NvWZ-Beilage 2021, 3 (6).

muss es möglich sein, im Falle von „Massenüberwachung" durch einen EMRK-Konventionsstaat einen wirksamen Rechtsbehelf einzulegen. Das Gericht führte dazu aus, dass die Verpflichtung, eine betroffene Person im Nachhinein über die Massenüberwachung zu unterrichten, eine geeignete Maßnahme darstelle, um zu beurteilen, ob ein Rechtsbehelf wirksam sei.[103] Einer vorherigen Benachrichtigung bedarf es jedoch nicht, wenn auch ohne diese ein Rechtsschutzbegehren möglich ist und eine materiell-rechtliche Prüfung des Begehrens erfolgen kann.[104] Dies muss jedoch auch tatsächlich gegeben sein.

Im Zusammenhang mit der automatisierten Auswertung von Massendaten und den zunehmenden Möglichkeiten, welche die Nutzung KI-basierter Systeme eröffnet, ist es hier zwingend notwendig, die oben beschriebenen Anforderungen von Fairness, Erklärbarkeit und Transparenz in allen Stadien der Nutzung solcher Systeme zu gewährleisten, und zwar bedarfsgerecht und akteurspezifisch.

4. Schlussfolgerungen und Ausblick

Dieser Beitrag hat gezeigt, dass die internationale Zusammenarbeit der Sicherheitsbehörden im großen Umfang eine Informationszusammenarbeit ist und daher im Kern auf Datenaustausch basiert. Grundlegende Prinzipien wie *Fairness*, *Transparenz, KI-Erklärbarkeit* und *Accountability* werden dabei oft vernachlässigt. Die weitreichenden Möglichkeiten der Datenauswertung mithilfe sich stetig entwickelnder KI-Anwendungen verschärfen diese Problematik in der Tendenz. Selbst innerhalb der EU mit ihrem vergleichsweise ausgeprägten Rechtsrahmen für die Zusammenarbeit von Polizeibehörden, der durch verbindliches EU-Recht, die EMRK und die dazu ergehende Rechtsprechung geprägt ist, bleibt die Annahme identischer rechtsstaatlicher Standards bisher mehr Wunsch als Wirklichkeit. Der in diesem Beitrag näher betrachtete *EncroChat*-Fall hat vielmehr erneut gezeigt, dass die transnationale Informationszusammenarbeit den Sicherheitsbehörden „Hintertüren" zur Umgehung rechtsstaatlicher Schutzstandards öffnet.

Die Rolle der EU in diesem Zusammenhang ist durchaus ambivalent. Einerseits werden mit der aktuellen Digitalrechtsgesetzgebung umfangrei-

103 CE:ECHR:2021:0525JUD005817013, Rn. 357.
104 Ebd.

che Regelungen bezüglich der Datenverarbeitung allgemein, aber auch ganz speziell bezüglich der Regulierung von KI unter Einbeziehung von Polizei und Strafjustiz neu geschaffen bzw. konkretisiert. Diese zielen auch auf eine stärkere Informationszusammenarbeit im öffentlichen wie im privaten Bereich ab. Andererseits tragen die europäischen Gerichte wie der EuGH und der EGMR aktiv dazu bei, den bestehenden konventionsrechtlichen Menschenrechtsschutz auch auf diese neuen Entwicklungen anzuwenden. Die fortwährenden Bestrebungen nach immer neuen Überwachungstechniken und Datenverarbeitungsmethoden zu Lasten des Grundrechtsschutzes, können so in Europa jedenfalls ein Stück weit eingehegt werden.

Bei der Informationszusammenarbeit der Sicherheitsbehörden außerhalb der EU bzw. zwischen EU- und Drittstaaten sind Standards wie *Fairness, Transparenz, KI-Erklärbarkeit* und *Accountability* bislang noch deutlich weniger ausgeprägt als innerhalb der EU. Zwar mag die EU auch hier – wie bereits bei der DSGVO – Vorbildcharakter für den Rechtsrahmen außerhalb der EU haben. Höhere und effektive Schutzstandards dürften aber kaum ohne zusätzliche verbindliche völkerrechtliche Regelungen etabliert werden können.

Literatur

Aden, Hartmut (2016): The Role of Trust for the Exchange of Police Information in the European Multi-level System**.** In: Delpeuch, Thierry und Ross, Jacqueline (Hrsg.), *Comparing the Democratic Governance of Police Intelligence. New Models of Participation and Expertise in the United States and Europe*. Cheltenham, UK: Edward Elgar Publishing, S. 322-334.

Aden, Hartmut (2018): Information Sharing, Secrecy and Trust among Law Enforcement and Secret Service Institutions in the European Union. *West European Politics (WEP)* 41(4), S. 981-1002.

Aden, Hartmut (2021): Europäische Rechtsgrundlagen und Institutionen des Polizeihandelns (= Abschnitt M). In: Lisken, Hans und Denninger, Erhard (Hrsg.): *Handbuch des Polizeirechts,* 7. Aufl. München: C.H. Beck, S. 1809-1905.

Aden, Hartmut; Schönrock, Sabrina; John, Sonja; Tahraoui, Milan und Kleemann, Steven (2022): Accountability-Vorkehrungen für die Erfüllung von Menschenrechtspflichten der Polizei bei der Nutzung Künstlicher Intelligenz. *Zeitschrift für Menschenrechte (zfmr),* 16(2), S. 50-72.

Article-29-Datenschutzgruppe (2016): Opinion 01/2016 on the EU–U.S. Privacy Shield draft adequacy decision, 16/EN WP 238 vom 16. April 2016. Brussels. URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf (besucht am 09. 05. 2023).

Arzt, Clemens (2021): Informationsverarbeitung im Polizei- und Strafverfahrensrecht (=Abschnitt G). In: Lisken, Hans und Denninger, Erhard (Hrsg.): *Handbuch des Polizeirechts,* 7. Aufl. München: C.H. Beck, Rn 1184-1189.

Bäuerle, Michael (2023): Elemente einer Europäischen Vision für die Regulierung von Big Data bei Polizei und Justiz. *Computer und Recht (CR)*, 49(1), S. 64-69.

Bellanova, Rocco; de Goede, Marieke (2022): The algorithmic regulation of security: An infrastructural perspective. *Regulation & Governance*, 16, S. 102-118.

Bignami, Francesca (2007): European Versus American Liberty: A Comparative Privacy Analysis of Anti-Terrorism Data-Mining. *Boston College Law Review 48,* S. 609-698.

Bignami, Francesca (2015): The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens. Study for the LIBE Committee, *GWU Law School Public Law Research Paper* No. 2015-54.

Bradford, Anu (2020): *The Brussels Effect: How the European Union Rules the World.* Oxford/New York: Oxford University Press.

Campbell. Duncan (2022): Two convicted in first murder plot case involving EncroChat messaging system. *The Guardian* vom 14. März 2022. URL: https://www.theguardian.com/world/2022/mar/14/two-guilty-of-james-bond-gun-plot-in-encrochat-conviction (besucht am 09. 05. 2023).

Canor, Iris (2013): Solange horizontal – Der Schutz der EU-Grundrechte zwischen Mitgliedstaaten. *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht (ZaöRV),* 73, S. 249-294.

Dehmel, Susanne; Ossmann-Magiera, Lea Ludmilla und Weiss, Rebekka (2023): Drittstaatentransfers nach Schrems II. *Multimedia und Recht (MMR) Zeitschrift für IT-Recht und Recht der Digitalisierung*, S. 17-22.

Derin, Benjamin und Singelnstein, Tobias (2021): Verwendung und Verwertung von Daten aus massenhaften Eingriffen in informationstechnische Systeme aus dem Ausland (Encrochat). *Neue Zeitschrift für Strafrecht (NStZ)*, S. 449-454.

Europäische Kommission (2021): Entwurf einer Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, COM(2021) 206 final, 2021/0106(COD).

Europäische Kommission (2022): Pressemitteilung vom 13.12.2022. URL: https://ec.europa.eu/commission/presscorner/detail/de/ip_22_7631 (besucht am 09. 05. 2023).

Europäischer Datenschutzausschuss (EDSA) (2020) Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen. URL: https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_de.pdf (besucht am 09. 05. 2023).

Europäischer Datenschutzausschuss (EDSA) (2021): Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten. URL: https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_de.pdf (besucht am 09. 05. 2023).

Europäischer Datenschutzausschuss (EDSA) (2023): Pressemitteilung vom 28.2.2023. URL: https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_de (besucht am 09. 05. 2023).

Europäischer Datenschutzbeauftragter (EDSB) (2020): Entscheidung vom 17.9.2020 – C 2019-0370. URL: https://edps.europa.eu/sites/edp/files/publication/20-09-18_edps_decision_on_the_own_initiative_inquiry_on_europols_big_data_challenge_en.pdf (besucht am 09. 05. 2023).

Europäischer Datenschutzbeauftragter (EDSB) (2021): Entscheidung vom 21.12.2021 – C 2021-0699. URL: https://edps.europa.eu/system/files/2022-01/22-01-10-edps-decision-europol_en.pdf (besucht am 09. 05. 2023).

Europäisches Parlament (2021): Exchanges of Personal Data after the Schrems II Judgment, PE 698.678. URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694678/IPOL_STU(2021)694678_EN.pdf (besucht am 09. 05. 2023).

Europäisches Parlament (2022): EncroChat's path to Europe's highest courts. URL: https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/739268/EPRS_ATA(2022)739268_EN.pdf (besucht am 09. 05. 2023).

Europarat (2020): Ad Hoc Committee on Artificial Intelleigence (CAHAI), Feasibility Study, CAHAI(2020)23, 17.12.2020.

European Network of Forensic Science Institutes (2021): Best Practice Manual for Digital Image Authentication, ENFSI-BPM-DI-03, 1. URL: https://enfsi.eu/wp-content/uploads/2022/12/1.-BPM_Image-Authentication_ENFSI-BPM-DI-03-1.pdf (besucht am 09. 05. 2023).

European Union Agency for Criminal Justice Cooperation (2020): Eurojust Pressemitteilung vom 2.7.2020. URL: https://www.eurojust.europa.eu/news/dismantling-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe (besucht am 09. 05. 2023).

Ewald, Uwe (2018): Digitale Beweismittel und neue Wege der Strafverteidigung. In: Strafverteidigervereinigungen, Organisationsbüro (Hrsg.): *Räume der Unfreiheit, Texte und Ergebnisse des 42. Strafverteidigertages*, Münster, 2.-4.3.2018.

Generalversammlung der Vereinten Nationen (2014): Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc. A/69/397, 23.09.2014.

Gonçalves, Anabela Susana de Sousa (2022): The ECtHR's Bosphorus Presumption and the European Union's principle of mutual trust. JusGov Research Paper No. 2022-05.

Glouftsios, Georgios; Leese Matthias (2023): Epistemic Fusion: Passenger Information Units and the making of international security, *Review of International Studies*, 49(1), S. 125-142.

Goodwin, Bill (2022): Police EncroChat cryptophone hacking implant did not work properly and frequently failed, *Computer weekly* vom 11. März 2022. URL: https://www.computerweekly.com/news/252514476/Police-EncroChat-cryptophone-hacking-implant-did-not-work-properly-and-frequently-failed (besucht am 09. 05. 2023).

Gressel, Céline und Orlowski, Alexander (2019): Integrierte Technikentwicklung: Herausforderungen, Umsetzungsweisen und Zukunftsimpulse. *TATuP – Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis*, 28(2), S. 71–72.

Haratsch, Andreas (2006): Die Solange-Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte – Das Kooperationsverhältnis zwischen EGMR und EuGH. *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht (ZaöRV),* 66, S. 927-947.

Hornung, Gerrit (2022): Künstliche Intelligenz zur Auswertung von Social Media Massendaten – Möglichkeiten und rechtliche Grenzen des Einsatzes KI-basierter Analysetools durch Sicherheitsbehörden. *Archiv des öffentlichen Rechts (AöR)*, 147(1), S. 1-69.

Huber, Bertold (2020): Das BVerfG und die Ausland-Ausland-Fernmeldeaufklärung des BND. *Neue Zeitschrift für Verwaltungsrecht (NVwZ-Beilage)*, S. 3-9.

Huber, Bertold (2021): „Massenüberwachung" vor dem EGMR. *Neue Zeitschrift für Verwaltungsrecht (NvWZ-Beilage)*, S. 3-10.

Iliadis, Andrew und Acker, Amelia (2022): The seer and the seen: Surveying Palantir's surveillance platform. *The Information Society*, 38(5), S. 334-363.

Kävrestad, Joakim (2020): *Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications*, 2. Aufl., Heidelberg: Springer.

Kipker, Dennis-Kenji (2021): Der Elefant im Raum: Aktuelle Diskussion um den Drittlandtransfer personenbezogener Daten. *Zeitschrift für Datenschutz (ZD)*, S. 397-398.

Kipker, Dennis-Kenji und Bruns, Hauke (2022): EncroChat und die „Chain of Custody". *Multimedia und Recht (MMR) Zeitschrift für IT-Recht und Recht der Digitalisierung*, S. 363-368.

Lavenex, Sandra (2007): Mutual recognition and the monopoly of force: limits of the single market analogy, *Journal of European Public Policy*, 14(5), S. 762-779.

Lowe, Mattew R. (2021): All Eyes on U.S.: Regulating the Use & Development of Facial Recognition Technology, *Rutgers Computer & Technology Law Journal,* 48(1), S. 1-50.

Mehrabi, Ninareh; Morstatter, Fred; Saxena, Nripsuta Ani; Lerman, Kristina und Galstyan, Aram (2021): A Survey on Bias and Fairness in Machine Learning. *ACM Computing Surveys (CSUR)*, 54,(6), Article 115, S. 1-35.

Menschenrechtsrat der Vereinten Nationen (2014): Concluding observations on the fourth periodic report of the United States of America, CCPR/C/USA/CO/4, 23.04.2014.

Menschenrechtsrat der Vereinten Nationen (2018): The right to privacy in the digital age, Report of the United Nations High Commissioner for Human Rights, A/HRC/39/29, 3.8.2018.

Menschenrechtsrat der Vereinten Nationen (2021): The right to privacy in the digital age - Report of the United Nations High Commissioner for Human Rights, A/HRC/48/31, 13.9.2021.

National Institute of Standards and Technology (NIST) (22. Nov. 2022): Digital and Multimedia Evidence. URL : https://www.nist.gov/spo/forensic-science-program/digital-and-multimedia-evidence (besucht am 09. 05. 2023).

O'Brien, Thomas C. und Tyler, Tom R. (2019): Rebuilding trust between police & communities through procedural justice & reconciliation. *Behavioral Science & Policy*, 5(1), S. 35–50.

OECD (2019): Empfehlung des Rats zu künstlicher Intelligenz, OECD/LEGAL/0449, 22.5.2019.

Pauli, Gerhard (2021): Zur Verwertbarkeit der Erkenntnisse ausländischer Ermittlungsbehörden – EncroChat. *Neue Zeitschrift für Strafrecht (NStZ)*, S. 146-149.

Pidoux, Jérémy (2022): Premiers contrôles par la Cour de cassation de procédures ouvertes à la suite de l'opération dite « EncroChat », *Dalloz actualité* vom 14. Nov. 2022. URL: https://www.dalloz-actualite.fr/flash/premiers-controles-par-cour-de-cassation-de-procedures-ouvertes-suite-de-l-operation-dite-encr#.ZBRPDISZOUk (besucht am 09. 05. 2023).

Quintel, Teresa (2022): The EDPS on Europol's Big Data Challenge in Light of the Recast Europol Regulation: The Question of Legitimizing Unlawful Practices. *European Data Protection Law Review (EDPL)*, 8(1), S. 90-102.

Raposo, Vera L. (2023): (Do not) remember my face: uses of facial recognition technology in light of the general data protection regulation. *Information & Communications Technology Law*, 32(1), S. 45-63.

Ruppert, Felix (2022): Erheben ist Silber, Verwerten ist Gold? Verwendbarkeit und Verwertbarkeit von Daten ausländischer Ermittlungsbehörden im Lichte des Grundrechtsschutzes – EncroChat. *Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht (NZWiSt)*, S. 221-227.

Rüß, Oliver und Lutz, Markus (2022): Die novellierte Europol-Verordnung: Eine europäische Antwort auf das FBI?. *Zeitschrift für das gesamte Sicherheitsrecht (GSZ),* S. 221-228.

Ryngaert, Cedric M.J. und van Eijk, Nico A.N.M. (2019): International Cooperation by (European) security and intelligence services: reviewing the creation of a joint database in light of data protection guarantees. *International Data Privacy Law*, 9(1), S. 61-73.

Schmahl Stefanie (2019): Intelligence and Human Rights. In: Dietrich, Jan-Hendrick und Sule Satish (Hrsg.): *Intelligence Law and Policies in Europe*, München, Bloomsbury, S. 291-334.

Schmahl, Stefanie (2020): Grundrechtsbindung der deutschen Staatsgewalt im Ausland. *Neue Juristische Wochenschrift (NJW)*, S. 2221-2224.

Staffler, Lukas (2016): Geheimdienstliches Verschwindenlassen von Terrorverdächtigen (extraordinary renditions) im Lichte der EGMR-Judikatur: der Fall Nasr (alias Abu Omr) und Ghali gegen Italien. *Europäische Grundrechte-Zeitschrift (EuGRZ)*, S. 344-352.

Stoykova, Adi (2021): Digital Evidence: Unaddressed threats to fairness and the presumption of innocence. *Computer Law & Security Review*, 42, S. 1-20.

Sunshine, Jason und Tyler, Tom R. (2003): The Role of Procedural Justice and Legitimacy in Shaping Public Support for Policing. *Law and Society Review*, 37(3), S. 513-548.

The White House (07. Okt. 2022): Federal Register, Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities Executive Order 14086., URL: https://www.govinfo.gov/content/pkg/FR-2022-10-14/pdf/2022-22531.pdf (besucht am 09. 05. 2023).

UNESCO Recommendation on the ethics of artificial intelligence, SHS/BIO/REC-AI-ETHICS/2021, 2021.

United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism (2014): Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc A/69/397.

United Nations Chief Executive Board (2022): Principles for the ethical use of artificial intelligence in the United Nations system, CEB/2022/2/Add.1, Chief Executives Board for Coordination Distr.: General 27.10.2022.

Venice Commission (2015): Report on the Democratic Oversight of Signals Intelligence Agencies adopted by the Venice Commission at its 102nd Plenary Session, Venedig 20.-21.3.2015, CDL-AD(2015)011.

Wexler, Rebecca (2021): Privacy Asymmetries: Access to Data in Criminal Defense Investigations. *UCLA Law Review*, 68(1), S. 212-287.