KOK

Bundesweiter Koordinierungskreis
gegen Menschenhandel e.V.

MENSCHENHANDEL 2.0 – DIGITALISIERUNG DES MENSCHENHANDELS IN DEUTSCHLAND

Entwicklungen und Handlungsoptionen

MENSCHENHANDEL 2.0 – DIGITALISIERUNG DES MENSCHENHANDELS IN DEUTSCHLAND

Entwicklungen und Handlungsoptionen

KOK
Bundesweiter Koordinierungskreis
gegen Menschenhandel e.V.

Angaben zur Autorin:

Dr. Dorothea Czarnecki hat in den letzten 17 Jahren in Praxis und Forschung zu Menschenhandel und sexueller Ausbeutung von Kindern in Lateinamerika, Europa und Südostasien gearbeitet. Sie hat ein Diplom in interkultureller Pädagogik und promovierte in Sozialwissenschaften zu Lebenswelten von Mädchen in sexueller Ausbeutung in Guatemala. Neben anderen führte Dorothea Czarnecki Forschung für die Europäische Kommission zu Handel mit Kindern in Deutschland durch, für ECPAT Deutschland e. V. zu reisenden Sexualstraftätern in Kambodscha, für UNICEF Vietnam zu Online-Kinderschutz und für den KOK e. V. zu sicherer Unterbringung von Menschenhandelsbetroffenen. Viele Jahre war sie die stellvertretende Geschäftsleitung von ECPAT Deutschland, die Vize-Vorsitzende des Vorstands von ECPAT International und bis 2021 die stellvertretende und Interims-Leitung des ECPAT-Sekretariats in Bangkok/Thailand. Seit 2022 ist Dorothea Czarnecki Analystin bei einem IT-forensischen Gutachterbüro und Beraterin der Initiative »ACT against child abuse« der Wilhelm von Humboldt Stiftung zur Vernetzung von Institutionen, die Hilfe für Menschen anbieten, die sich sexuell zu Kindern hingezogen fühlen.

ZUSAMMENFASSUNG

Technologischer Fortschritt in Form von Digitalisierung, befördert durch die Auswirkungen der Covid-19-Pandemie, wird auch von Menschenhändler*innen genutzt, die nun mit einer größeren Reichweite, ortsunabhängig und mit weniger Risiko der Aufdeckung ihren kriminellen Machenschaften nachgehen können. Menschenhändler*innen bedienen sich des Internets und weiterer Informations- und Kommunikationstechnologien (IKTs) in jeder Phase des Ausbeutungsprozesses – insbesondere bei der Anwerbung neuer potenzieller Opfer über soziale Netzwerke – sowie auch zur Kontrolle Betroffener während und zur Druckausübung nach der Ausbeutung. Die vorliegende Studie veranschaulicht anhand unterschiedlicher Fallbeispiele die Vielzahl von Möglichkeiten, wie Täter*innen dabei vorgehen. Anders als allgemeinhin vielleicht vermutet spielen dabei das Darknet und Kryptowährungen nur eine untergeordnete Rolle.

Auf EU-Ebene befinden sich neue rechtliche Instrumente als Reaktion auf die Digitalisierung des Menschenhandels zum Großteil erst in der Entwicklung, mit besonderer Beachtung einer bisher nie da gewesenen verpflichtenden Inverantwortungnahme von Online-Plattformbetreibern. Obwohl Strafverfolgung, Justiz und spezialisierte Fachberatungsstellen für Betroffene des Menschenhandels in Deutschland darüber hinaus kaum Gesetzeslücken benennen, die unter Berücksichtigung technologischer Komponenten die Strafverfolgung von Menschenhandelsfällen oder die Unterstützung der Betroffenen verhindern oder erschweren würden, sehen sie sich mit neuen Herausforderungen konfrontiert. Ein gesellschaftliches als auch behördliches Bewusstsein für das Thema digitale und technologiegestützte Gewalt in all seinen Ausprägungen ist noch nicht umfassend vorhanden, und damit haben Strafverfolgungsbehörden und auch Fachberatungsstellen bisher noch nicht flächendeckend die Notwendigkeit gesehen, Kompetenzen in diesem Bereich auf- oder auszubauen. Es sind kaum technische Fähigkeiten vorhanden, um angemessen auf technologische Herausforderungen bzgl. IT-Sicherheit und den digitalen Modus Operandi der Menschenhändler*innen zu reagieren. Auch der von Unsicherheiten geprägte Umgang mit digitaler Beweissicherung stellt in der Praxis eine große Hürde für Betroffene in Bezug auf den Zugang zu ihren Rechten auf Gewaltschutz dar.

Um die Schutzlücken für Betroffene zu schließen, arbeiten verschiedene Akteur*innen an technologiegestützten Lösungsansätzen. Die Studie stellt vier davon vor, die auf unterschiedlichen technologischen Konzepten basieren (Website, Machine Learning, virtuelle Realität und App).

Darüber hinaus wird auf Grundlage der herausgearbeiteten Hindernisse und Hürden in der Praxis an Politik, Strafverfolgung und Fachberatungsstellen appelliert,

- die Cybersicherheitsagenda um Menschenhandel zu erweitern und eine einheitliche Definition einzuführen,
- die Digitalisierung der Behörden zügig voranzutreiben,
- Zuständigkeiten für das Thema technologiegestützter Menschenhandel zu klären und multidisziplinäre Zusammenarbeit zu erleichtern,
- Technologieunternehmen rechtlich in die Verantwortung zu nehmen,
- IT-Infrastruktur bei der Finanzierung von Fachberatungsstellen zu berücksichtigen,
- Sensibilität zur Thematik, IT-Kompetenzen und Ressourcen auszubauen,
- IT-Sicherheit zu erhöhen und IKT-Schutzkonzepte zu erweitern.

INHALTSVERZEICHNIS

1

EINLEITUNG

32 Jahre nach der Einführung des Internets zur kommerziellen weltweiten Nutzung haben geschätzt 66,2 Prozent der Weltbevölkerung Zugang zum Internet. Das bedeutet: 4,9 Milliarden Menschen nutzen das Internet, Tendenz steigend.[1] In Deutschland nutzen 92 Prozent der Bevölkerung das Internet und weitere Informations- und Kommunikationstechnologien (IKTs).[2] Unter IKTs werden technische Hilfsmittel verstanden, die zum Übertragen, Speichern, Erstellen, Teilen oder Austauschen von Informationen verwendet werden. Sie umfassen Computer, Internet (Websites, Blogs und E-Mails), Live-Übertragungstechnologien (Radio, Fernsehen und Webstreaming), aufgezeichnete Übertragungstechnologien (Podcasting, Audio- und Videoplayer) und Telefonie (Festnetz oder Mobilfunk, Satellit, Videokonferenz).[3] Zum weiteren digitalen Umfeld in diesem Kontext zählen u. a. digitale Netzwerke, Inhalte, Dienste und Anwendungen, vernetzte Geräte und Umgebungen, virtuelle und erweiterte Realitäten (*virtual reality*, *augmented reality*), künstliche Intelligenz, Robotik, automatisierte Systeme und Algorithmen.[4]

Die Covid-19-Pandemie und die damit einhergehenden Lockdowns seit Frühjahr 2020 können als Beschleuniger der Digitalisierung gesehen werden. Selbst ehemals skeptische Nutzer*innen digitaler Technologien waren auf ihren Gebrauch angewiesen, sei es durch remote Zusammenarbeit mit Arbeitskolleg*innen, durch Onlineunterricht der Schulen und Universitäten oder zur mentalen Entlastung durch das Aufrechterhalten sozialer Kontakte online. Doch dieser Digitalisierungsschub wurde nicht nur für positive Zwecke genutzt: »Insbesondere die Auswirkungen der COVID-19-Pandemie auf die Cyberkriminalität haben weltweit eine ›neue Normalität‹ geschaffen. Die Entwicklungen im Bereich der Cyberkriminalität haben das Verhalten von Kriminellen verändert, um die aktuelle Krise auszunutzen [...] und zeigen, dass Cyberkriminelle bereit sind, ihre Arbeitsweise so anzupassen, dass sie menschliche und technologische Schwachstellen ausnutzen können.« [5]

Menschenhändler*innen haben ihre Geschäftsmodelle den Gegebenheiten angepasst und werben Betroffene online oder mittels IKTs an, beuten sie aus und kontrollieren sie.[6] Menschenhandel ist nach wie vor eine der profitabelsten kriminellen Tätigkeiten. In der EU werden die Einnahmen der Straftäter*innen aus dem Menschenhandel zum Zwecke der sexuellen Ausbeutung – dem häufigsten

1 Statista.de: Statistiken zur Internetnutzung weltweit: https://de.statista.com/themen/42/internet/#dossierKeyfigures.

2 Statista.de: Anteil der Internetnutzer in ausgewählten Ländern in Europa im Jahr 2021: https://de.statista.com/statistik/daten/studie/184636/umfrage/internetreichweite-anteil-der-nutzer-in-europa/.

3 UNICEF, 2022: Legislating for a digital age, Glossary.

4 Kinderrechte.digital – Allgemeine Bemerkung Nr. 25 (2021) Über die Rechte der Kinder im digitalen Umfeld.

5 Phillips, K./Davidson, J. C./Farr, R. R./Burkhardt, C./Caneppele, S./Aiken, M. P.: Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. In: Forensic Sciences 2022-2, S. 394, eigene Übersetzung.

6 United Nations Office on Drugs and Crime (UNODC), 2021: The effects of the Covid 19 pandemic on trafficking in persons and responses to the challenges.

Zweck des Menschenhandels – in einem einzigen Jahr auf etwa 14 Mrd. EUR geschätzt.[7] Vor diesem Hintergrund ist nicht verwunderlich, dass organisierte Strukturen des Menschenhandels ihre Machenschaften zügig an neue Gegebenheiten adaptieren, wie beispielsweise die humanitäre Krise als Resultat des Ukrainekriegs ab Februar 2022 gezeigt hat. Frauen und ihre Kinder sollten auf Social-Media-Plattformen wie Facebook unter dem Deckmantel vermeintlicher Hilfsangebote in die Prostitution in Aufnahmeländern, unter anderem auch Deutschland, gelockt werden.[8]

Gleichzeitig werden die wirtschaftlichen Kosten, die der Menschenhandel jährlich in der EU verursacht, auf 2,7 Mrd. EUR geschätzt.[9] Neben einer finanziellen Mehrbelastung für Staaten ergeben sich aus internationalen Instrumenten menschenrechtliche Verpflichtungen zum Schutz und zur Unterstützung der Opfer und zur strafrechtlichen Ahndung der Täter*innen, allen voran sind die Europaratskonvention gegen Menschenhandel (SEV 197) und die EU-Richtlinie zur Verhütung und Bekämpfung des Menschenhandels und zum Schutz seiner Opfer (2011/36/EU) zu nennen. Anzumerken ist allerdings, dass diese Instrumente vor über zehn Jahren verfasst worden sind, als das Internet noch keine solche Rolle im Menschenhandel gespielt hat bzw. gewisse technische und technologische Möglichkeiten überhaupt noch nicht existierten.[10] Auch in der Praxis halten die Reaktionen des Unterstützungssystems für Betroffene, Strafverfolgung und Justiz in der Regel nicht mit dem Tempo des technologischen Fortschritts und gesellschaftlicher Veränderungen mit. So erschwerte die Covid-Pandemie Betroffenen den Zugang zu allen drei Bereichen, und die Digitalisierung des Menschenhandels stellte die Strafverfolgung vor große Herausforderungen.[11]

Zwei Jahre nach Beginn der Pandemie und damit der allgemeinhin erweiterten Nutzung digitaler Möglichkeiten stellt sich die Frage, inwieweit auch eine technologische Anpassung spezifisch im Akteursfeld der Menschenhandelsbekämpfung und Unterstützung der Betroffenen erfolgt ist. Bisher existieren nur anekdotische Hinweise darauf, wie sich die Situation in Deutschland bzgl. des Einflusses und der Auswirkungen des Internets auf Menschenhandel gestaltet (siehe Kapitel 3). Eine wissenschaftlich und praktisch fundierte Betrachtung des Phänomens fehlt.

1.1 BEGRIFFSKLÄRUNG MENSCHENHANDEL

Die vorliegende Studie befasst sich mit Menschenhandel gemäß der Definition des KOK,[12] die weiter gehalten ist als die Paragrafen § 232–233a Strafgesetzbuch. Menschenhandel liegt demnach dann vor, wenn Personen mittels Täuschung, Drohungen, Gewaltanwendung angeworben werden und im Zielland zur Aufnahme und Fortsetzung von Dienstleistungen und Tätigkeiten gebracht oder gezwungen werden, die ihre verbrieften Menschenrechte verletzen, indem sie ausbeuterisch oder sklavenähnlich sind. Dabei muss die Anwerbung nicht unbedingt im Ausland erfolgen, sondern das Ausnutzen der Hilflosigkeit im Zielland fällt auch unter den Menschenhandelsbegriff. Kernelemente sind vielmehr Nötigung, Zwang und Täuschung, wobei Zwang verschiedene Formen annehmen kann. Er kann durch direkte physische Gewalt oder durch Androhung derselben, Erpressung, unrechtmäßiges Einbehalten von Dokumenten und verdientem Geld, Raub, Isolation und Betrug ausgeübt werden. Auch das Ausnutzen einer hilflosen Lage z. B. aufgrund des Aufenthaltes im Ausland, der Autoritätsmissbrauch und die Schuldknechtschaft sind Formen des Zwangs bei Menschenhandel und Ausbeutung.

Bisher lässt diese Begriffsklärung den Einsatz von Informations- und Kommunikationstechnologien unbeachtet.

7 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. Die Strategie der EU zur Bekämpfung des Menschenhandels 2021–2025, COM(2021) 171 final, 14.4.2021, S. 7., mit Verweis auf: European Commission, 2021: Mapping the risk of serious and organised crime infiltration in legitimate businesses. https://data.europa.eu/doi/10.2837/64101.

8 Organization for Security and Co-operation in Europe (OSCE), 2022: Recommendations on enhancing efforts to identify and mitigate risks of trafficking in human beings online as a result of the humanitarian crisis in Ukraine.

9 European Commission, 2020: Study on the economic, social and human costs of trafficking in human beings within the EU.

10 Das Europäische Parlament hat inzwischen eine Evaluierung der Richtlinie 2011/36 in Auftrag gegeben, die Ergebnisse werden für Dezember 2022 erwartet. Es wird davon ausgegangen, dass eine Überarbeitung der Richtlinie angestrebt wird. Das Thema Digitalisierung im Menschenhandel wird vermutlich hierbei ebenfalls eine Rolle spielen, in welchem Umfang und mit welchen Maßnahmen es aufgenommen wird, ist jedoch zum Zeitpunkt der Erarbeitung dieser Studie noch unklar.

11 Vgl. MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN. Die Strategie der EU zur Bekämpfung des Menschenhandels, COM(2021) 171 final, 14.04.2021.

12 Vgl. KOK-Begriffsklärung: https://www.kok-gegen-menschenhandel.de/menschenhandel/was-ist-menschenhandel.

1.2 FRAGESTELLUNGEN UND ZIEL

Die Fachberatungsstellen des Bundesweiten Koordinierungskreises gegen Menschenhandel – KOK e. V. haben die Notwendigkeit erkannt, neue Kenntnisse um die Digitalisierung des Menschenhandels zu erwerben. Sie möchten die Lücke zwischen dem bisher benötigten Wissen um »klassisch-analoge« Fälle des Menschenhandels und technologischen Entwicklungen, die neue digitale und IT-Kompetenzen erforderlich machen, schließen. Aus diesem Grund hat der KOK die vorliegende Studie in Auftrag gegeben, um erste Einblicke und Antworten zu erhalten, wie sich Informations- und Kommunikationstechnologien auf Menschenhandelsfälle in Deutschland auswirken, welche Konsequenzen und Herausforderungen sich daraus für spezialisierte Fachberatungsstellen für Betroffene des Menschenhandels als auch für Justiz und Strafverfolgung ergeben und welches notwendige Handlungsschritte und Empfehlungen für Politik, Strafverfolgung, Justiz und die Fachberatungsstellen sind. Die Studie zielt darauf ab, die Beratungslandschaft zum Thema Menschenhandel in Deutschland sowie weitere Fachakteur*innen, die sich mit dem Thema befassen, zu informieren und zu sensibilisieren. Angesichts bisher fehlender Publikationen zu diesem Thema in Deutschland kann die vorliegende Studie als Grundlagenpapier betrachtet werden.

1.3 VORGEHENSWEISE

In Übereinstimmung mit den Grundsätzen und dem Mandat des KOK stellt die vorliegende Studie die Bedarfe und Perspektive der spezialisierten Fachberatungsstellen in Deutschland in den Mittelpunkt, die Betroffene von Menschenhandel und Ausbeutung unterstützen. Die Mehrzahl der für diese Studie geführten Expert*inneninterviews fand aus diesem Grund mit Beraterinnen aus Fachberatungsstellen in Deutschland statt. Im Zeitraum vom 05. Juli bis 01. September 2022 wurden insgesamt zehn halbstrukturierte Interviews durchgeführt: sechs mit Praktikerinnen aus (Fach-)Beratungsstellen, eines mit dem Bundeskriminalamt – Abteilung Menschenhandel, eines mit der auf Menschenhandel spezialisierten Staatsanwaltschaft Berlin, ein Interview mit zwei Analysten eines IT-forensischen Gutachterbüros und eines mit einem Vertreter der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE), um die internationale Perspektive einzubinden. Eine Interviewübersicht befindet sich im Anhang.

Jedes Interview wurde transkribiert und anhand vorher definierter Kategorien ausgewertet. Die Kategorienerstellung basierte auf einer Literaturrecherche in Deutschland und im internationalen Raum. Da die Studie zum Ziel hat, spezifisch die Situation in Deutschland zu beleuchten, wurden nur internationale Informationen herangezogen, die auch für den deutschen Kontext relevant scheinen oder wenn in Deutschland keine verlässlichen Daten und gesicherten Informationen für die gesetzte Fragestellung zu finden waren. Die vorliegende Publikation versteht sich als explorative Studie zur Digitalisierung des Menschenhandels als ein bisher kaum wissenschaftlich untersuchtes Themenfeld in Deutschland. Sie liefert erste Erkenntnisse, hat jedoch aufgrund ihres vorgegebenen Umfangs und der geringen Anzahl von Expert*inneninterviews nur eine limitierte Aussagekraft. Es wäre wünschenswert, wenn sie als Grundlage für weitere Forschung und als Ansatzpunkt für eine politische Auseinandersetzung mit dem Thema Digitalisierung des Menschenhandels in Deutschland dienen würde.

1.4 THEMATISCHE AUSLASSUNG UND ABGRENZUNG: MISSBRAUCHSABBILDUNGEN VON KINDERN UND LIVESTREAMING SEXUALISIERTER GEWALT

Online-Missbrauchsabbildungen von Kindern und Jugendlichen durch Fotos, Videos, animierte Darstellungen und Livestreamings sexualisierter Gewalt werden in Deutschland strafrechtlich gesondert von Menschenhandel als sexueller Missbrauch von Kindern und Kinderpornografie behandelt und sind daher nicht Untersuchungsgegenstand dieser Studie. Menschenhandel mittels digitaler Technologien und insbesondere Livestreamings sexualisierter Gewalt gegen Kinder können durchaus Überschneidungsflächen aufzeigen, allem voran durch eine kommerzielle Ausbeutungskomponente. Dies erkennt auch die allgemeine Bemerkung Nummer 25 (2021) des Kinderrechtsausschusses der Vereinten Nationen an, die erstmalig Kinderrechte im digitalen Umfeld thematisieren. [13] Demnach sei sexuelle Ausbeutung und Handel mit Kindern ein mögliches Risiko für Kinder im digitalen Umfeld.[14] Gleichzeitig brauche es jedoch für Prävention, Bekämpfung und Opferunterstützung eine umfangreiche Anstrengung im Rahmen nationaler Kinderschutzpolitiken.[15]

Erste Diskussionen in diesem Kontext haben sowohl auf internationaler Ebene als auch in Deutschland bereits stattgefunden und etliche Fragestellungen aufgeworfen, die einer tieferen Auseinandersetzung bedürfen: So gestalten sich Fälle von Menschenhandel in der Regel als schwierig zu ermitteln und juristisch zu verfolgen, mit einer nach wie vor geringen Verurteilungsrate. Bei sexuellem Kindesmissbrauch und Straftaten im Kontext von Missbrauchsabbildungen von Kindern bestehen rechtliche Möglichkeiten von Therapieauflagen gegen die Täter*innen, die bei Menschenhandelsfällen nicht vorgesehen sind. Darüber hinaus beinhaltet Menschenhandel neben sexueller Ausbeutung auch andere Ausbeutungsformen (Zwangsarbeit, Organhandel, erzwungene Bettelei, Ausnutzen strafbarerer Handlungen), die keine Verbindung zu Livestreaminghaben. Zudem dürfte die Einbeziehung sexualisierter Gewalt an Kindern mittels IKTs in gesetzliche Regelungen zu Menschenhandel nicht dazu führen, dass die sexuellen und kindspezifischen Aspekte der Straftaten und die damit verbundenen Auswirkungen auf betroffene Kinder in den Hintergrund rücken oder Präventionsmaßnahmen behindern.[16]

Ein politisch bedeutsamer Schritt war die Setzung des Themas »Menschenhandel und Ausbeutung von Kindern online und offline« im Abschlusskomuniqué der G7-Staaten vom 28. Juni 2022.[17] Seitdem finden auf Ebene der Innenministerien und Strafverfolgungsbehörden der G7-Staaten Diskussionen und Austausch um mögliche Schnittflächen dieser Themenbereiche statt, mit dem Ziel einer effektiveren Strafverfolgung und eines besseren Opferschutzes. Empfehlungen sollen im November 2022 von den G7-Innenminister*innen verhandelt werden, weitere Beschäftigung sowohl national als auch international mit diesen Themenfeldern sind ausstehend.

13 Allgemeine Bemerkung 25 (2021) Über die Rechte der Kinder in Bezug auf das digitale Umfeld.

14 Vgl. ebd., Artikel 82: Die Vertragsstaaten sollen Kinder vor Gewalt im digitalen Umfeld mithilfe legislativer und behördlicher Maßnahmen schützen, einschließlich der regelmäßigen Überprüfung, Aktualisierung und Durchsetzung umfassender gesetzlicher, regulatorischer und institutioneller Rahmenbedingungen, die Kinder vor bekannten und neu auftretenden Gefahren durch alle Formen von Gewalt im digitalen Umfeld schützen. Solche Gefahren umfassen u. a. physische und psychische Gewalt, Verletzung oder Missbrauch physischer oder psychischer Art, Vernachlässigung oder Misshandlung, sexuelle Ausbeutung und sexuellen Missbrauch, Kinderhandel, geschlechtsspezifische Gewalt, Cyberaggression, Cyberangriffe und Informationskriegsführung. Die Vertragsstaaten sollen Sicherheits- und Schutzmaßnahmen im Einklang mit den sich entwickelnden Fähigkeiten des Kindes umsetzen.

15 Vgl. ebd., Artikel 25: Der Schutz von Kindern im digitalen Umfeld soll in die nationale Kinderschutzpolitik aufgenommen werden. Die Vertragsstaaten sollen Maßnahmen einführen, mit denen Kinder vor Gefahren geschützt werden, darunter auch vor Cyberaggressionen sowie digital unterstützter und im Internet stattfindender sexueller Ausbeutung und Misshandlung von Kindern. Sie sollen die Verfolgung solcher Delikte sicherstellen und Kindern, die so behandelt wurden, Abhilfe und Unterstützung gewährleisten.

2

MENSCHENHANDEL IM ZUSAMMENHANG MIT DEM INTERNET – VERSTÄNDNIS IN DER PRAXIS UND ANGRENZENDE BEGRIFFSKLÄRUNGEN

2.1 VERSTÄNDNIS IN DER PRAXIS – STATUS QUO

In Deutschland scheinen sich in der Arbeit der Fachakteure bisher noch keine gängigen Begrifflichkeiten durchgesetzt zu haben, welche die Digitalisierung des Menschenhandels abdecken. Die befragten Expert*innen nutzen weit gefasste Beschreibungen wie »Rolle des Internets im Menschenhandel« und »Menschenhandel im Zusammenhang mit dem Internet«, mit dem einstimmigen Hinweis, dass es bisher auch kaum die Notwendigkeit für Diskussionen und Austausch innerhalb ihrer Institutionen oder mit Kooperationspartnern gäbe. Die Relevanz scheint in der Praxis noch nicht groß genug, gesonderte Begrifflichkeiten zu besprechen. Wenn Fälle auftauchen, findet eine separierte Betrachtung einzelner Aspekte statt, z. B. welche Plattformen wurden für die Anwerbung der Betroffenen genutzt. Zurückzuführen ist das weniger darauf, dass keine Fälle in der Beratungspraxis vorkämen, sondern vielmehr auf die interne Einordnung und das sich noch zu entwickelnde Verständnis der Fachberatungsstellen bzgl. Informations- und Kommu-

16 Vgl. WeProtect Global Alliance, 2021: Framing Child Sexual Abuse and Exploitation Online as a Form of Human Trafficking: Opportunities, Challenges and Implications. Expert Roundtable Outcomes Briefing; ECPAT Deutschland e. V. und International Justice Mission Deutschland e. V.: Interdisziplinäres Fachgespräch zur sexuellen Ausbeutung von Kindern per Livestream, Mai 2022.

17 Kommuniqué der G7 Staats- und Regierungschefs, Arbeitsübersetzung, 28.06.2022, S. 32: Wir verpflichten uns, den Kampf gegen den Menschenhandel und unsere Bemühungen zur Verhütung und Bekämpfung sexuellen Missbrauchs und sexueller Ausbeutung von Kindern weltweit zu verstärken, sowohl online als auch offline. Wir ersuchen unsere Innenministerinnen und -minister, die Umsetzung des Aktionsplans zur Bekämpfung der sexuellen Ausbeutung und des sexuellen Missbrauchs von Kindern von September 2021 an voranzutreiben.

nikationstechnologien und Social Media. »Ich wäre mir des Themas nicht so bewusst gewesen, hätten wir da nicht jetzt darüber gesprochen. Es läuft zwar immer mit und wird immer mehr, aber wir haben uns da noch nie explizit Gedanken darüber gemacht« (Interview FBS).

Alle befragten Fachberatungsstellen stellten eigene Informationslücken und einen Mangel an Vertrautheit im Umgang mit Informations- und Kommunikationstechnologien im Allgemeinen und mit Aspekten der Digitalisierung des Menschenhandels im Speziellen fest. Bei der Anfrage für die vorliegende Studie kamen beispielsweise Fragen innerhalb des Teams einer Fachberatungsstelle zu grundlegenden Konzepten auf: Was versteht man unter Informations- und Kommunikationstechnologien? Was ist gemeint mit technologiegestützt? »Da sind wir sicher eher unbeholfen. […] Bei der Anfrage war meine Vorstellung zunächst, einen rein digitalen Menschenhandelsfall haben wir gar nicht. Dann aber habe ich erkannt: Es geht um Mischformen. Das ist, glaube ich, die Kunst, zu erkennen, dass es auch schon dazugehört« (Interview FBS). Doch gleichzeitig haben alle Fachberatungsstellen eine große Bereitschaft gezeigt, diese Lücken zu schließen. Sie sehen die Notwendigkeit für Sensibilisierung und Schulung der Beratungslandschaft von Grund auf: »Viele Beraterinnen sind unwissend und überrascht, was alles passieren kann. Wir alle müssen überhaupt erst auf Stand gebracht werden, was da so alles geschieht« (Interview FBS). Dann erst könnten angemessene Begrifflichkeiten ausdiskutiert werden.

Hier gibt es großen Nachholbedarf, denn unterschiedliche Begriffe im nationalen und internationalen Kontext bringen divergierende Konzepte und Verständnisse der Thematik in der zwischenstaatlichen und behördenübergreifenden Zusammenarbeit mit sich. Wie schon im »Terminologischen Leitfaden für den Schutz von Kindern vor sexueller Ausbeutung und sexualisierter Gewalt«[18] festgestellt wurde, und ebenso geltend für die sich gerade in Entwicklung befindenden Begriffswelten zu Menschenhandel im Zusammenhang mit dem Internet, kann der »[…] inkonsistente Gebrauch von Sprache und Begriffen […] zu widersprüchlichen Gesetzen und politischen Antworten auf ein und dasselbe Thema führen. […] Selbst dort, wo die gleichen Begriffe verwendet werden, gibt es häufig Meinungsunterschiede über deren tatsächliche Bedeutung, was dazu führt, dass die gleichen Worte benutzt werden, um sich auf unterschiedliche Handlungen oder Situationen zu beziehen. Dies hat beträchtliche Herausforderungen für die Weiterentwicklung und Planung von Politiken und Programmen, für die Weiterentwicklung von Rechtsvorschriften sowie für die Datenerfassung verursacht […]« (ECPAT International 2018, S. XIII).

2.2 ANGRENZENDE BEGRIFFSKLÄRUNGEN

Das »Zusatzprotokoll zur Verhütung, Bekämpfung und Bestrafung des Menschenhandels, insbesondere des Frauen- und Kinderhandels zum Übereinkommen der Vereinten Nationen gegen die grenzüberschreitende organisierte Kriminalität« (Palermo-Protokoll, 2000) als Grundlagenabkommen in der Bekämpfung des Menschenhandels hat eine international anerkannte Definition des Phänomens gegeben, die sich seit seiner Verabschiedung etabliert hat und in nationale Gesetzgebungen übernommen wurde.

Bisher fehlt ein vergleichbares Dokument, welches die technologiebasierten Komponenten, derer sich Menschenhandel im digitalen Umfeld bedient, abdecken würde. Selbst neuere fachspezifische Publikationen wie das Menschenhandels-Glossar des Ostseerats (2019) beinhalten

18 ECPAT International, 2018: Terminologischer Leitfaden für den Schutz von Kindern vor sexueller Ausbeutung und sexualisierter Gewalt.

keinerlei Nennung von Informations- und Kommunikationstechnologien oder sonstigen digitalen Aspekten, sondern beziehen sich lediglich auf »Offline-Menschenhandel«.[19] Angesichts dieser Lücke scheint es angemessen, die Auseinandersetzung um Konzepte der Digitalisierung von Straftaten zu erweitern und den Menschenhandel unter Verwendung von Informations- und Kommunikationstechnologien darin zu verorten.

2.2.1 Cyberkriminalität/Cybercrime

Das bisher relevanteste völkerrechtliche Abkommen im hier diskutierten Kontext ist das Übereinkommen des Europarats über Computerkriminalität (Budapest-Konvention, 2001) inkl. seines zweiten Zusatzprotokolls (2022), das als Reaktion auf den technologischen Fortschritt entwickelt worden ist.[20] Deutschland hat die Konvention 2001 unterzeichnet und am 09. März 2009 ratifiziert.[21] Die Intention der Budapest-Konvention ist die Implementierung eines international akzeptierten Rahmens rechtlicher Prinzipien und eines Klassifikationsschemas von Delikten im Zusammenhang mit Cybercrime. Allerdings zeigt eine Untersuchung aus dem Jahr 2022, dass es weiterhin an einer universell akzeptierten und präzisen Definition von Cybercrime fehlt.[22] Für die effektive Bekämpfung von Cybercrime ist jedoch eine allgemein akzeptierte Definition notwendig. Schwierigkeiten in der Klassifizierung von Cybercrime verhindern die Einführung spezifischer Straftatbestände, so die Autor*innen, was zu erheblichen Herausforderungen für Polizei und Justiz aufgrund eines limitierten Verständnisses und limitierter Reaktionsfähigkeit führe.[23] Die Untersuchung konnte weltweit keine Rechtsprechung identifizieren, die sich auf Cybercrime als eine spezifische Straftat beziehen würde.

Ähnlich der Legitimation des Terminologischen Leitfadens spricht sich die Untersuchung für die Erstellung eines gemeinsamen Lexikons für politische Entscheidungsträger*innen und die Praxis zur Klärung und Umsetzung einer gemeinsamen Sprache auf internationaler Ebene aus, da eine gemeinsame Sprache ein Schlüsselelement für die allgemeine Akzeptanz von Konzepten der Cyberkriminalität sei.[24] Als Grundlage dafür haben die Autor*innen den Versuch unternommen, auf Basis führender englischsprachiger Literatur eine Typologie des behandelten Phänomens herauszuarbeiten (siehe Abbildung 1).[25] Darin unterscheiden sie zunächst zwischen den zwei groben Kategorien cyber-abhängige und cyber-gestützte Verbrechen. Cyber-abhängig bedeutet, das Verbrechen basiert auf der Nutzung des Internets und könnte ohne Internet nicht existieren.

19 Council of the Baltic Sea States, Task Force against Trafficking in Human beings, 2019: Human Trafficking Glossary.

20 Cybercrime Convention Committee (T-CY), Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. Explanatory Report, 17.11.2021, Artikel 5: Die Informations- und Kommunikationstechnologie hat Gesellschaften weltweit auf außergewöhnliche Weise verändert, seit das Übereinkommen 2001 zur Unterzeichnung aufgelegt wurde. Seither hat jedoch auch die kriminelle Nutzung von Technologie erheblich zugenommen. Cyberkriminalität wird heute von vielen Parteien als ernsthafte Bedrohung der Menschenrechte, der Rechtsstaatlichkeit und des Funktionierens demokratischer Gesellschaften angesehen. Die Bedrohungen durch Cyberkriminalität sind zahlreich. Beispiele dafür sind sexuelle Online-Gewalt gegen Kinder und andere Straftaten gegen die Würde und Unversehrtheit von Personen, Diebstahl und Missbrauch personenbezogener Daten, die sich auf das Privatleben von Personen auswirken, Eingriffe in Wahlen und andere Angriffe auf demokratische Einrichtungen, Angriffe auf kritische Infrastrukturen wie verteilte Denial-of-Service-Angriffe und Ransomware-Angriffe oder der Missbrauch solcher Technologien für terroristische Zwecke. In den Jahren 2020 und 2021 verzeichneten Länder während der Covid-19-Pandemie signifikante Covid-19-bezogene Cyberkriminalität.

21 Stand der Unterzeichnungen und Ratifizierungen auf der Website des Europarats. https://www.coe.int/de/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=5isnGr2b.

22 Phillips, K./Davidson, J. C./Farr, R. R./Burkhardt, C./Caneppele, S./Aiken, M. P.: Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. In: Forensic Sciences 2022, 2, 379–398.

23 Vgl. ebd., S. 391.

24 Vgl. Ebd., S. 394.

25 Vgl. Ebd., S. 383.

Wenn man bei cyber-gestützten Verbrechen hingegen das Internet wegnimmt, geschehen diese Verbrechen zwar immer noch, aber auf einer viel lokaleren und eingeschränkten Ebene.

Diesen zwei Kategorien sind vier Modi Operandi untergeordnet, die jeweils unterschiedliche Zielgruppen, Motivation von Täter*innen und Taktiken zur Viktimisierung der Opfer umfassen:

I) Verbrechen gegen die Maschine richten sich sowohl gegen Daten und Systeme als auch gegen Staaten, beispielsweise *hacking* oder das Ausspionieren von Daten für politische Zwecke;
II) Verbrechen mit der Maschine, die meist Angriffe auf Vermögen oder Diebstahl zum Ziel haben, zum Beispiel Betrug;
III) Verbrechen in der Maschine, die auf zwischenmenschliche, sexualisierte und Gewalt gegen Gruppen zielen, worunter auch Ausprägungen des Menschenhandels zur sexuellen Ausbeutung, sexuelle Missbrauchsdarstellungen von Kindern und Verbrechen über Social-Media-Plattformen fallen;
IV) Cyber-unterstützte Verbrechen, die auf einen gelegentlichen Einsatz von Technologien bauen, d. h. Technologien zwar zu der Organisierung und Durchführung des beabsichtigten Verbrechens nutzen, doch das Verbrechen auch ohne deren Anwendung stattfinden würde, beispielsweise Drogenhandel und eben auch Menschenhandel – oder wenn ein*e Mörder*in das Entsorgen einer Leiche googelt.[26]

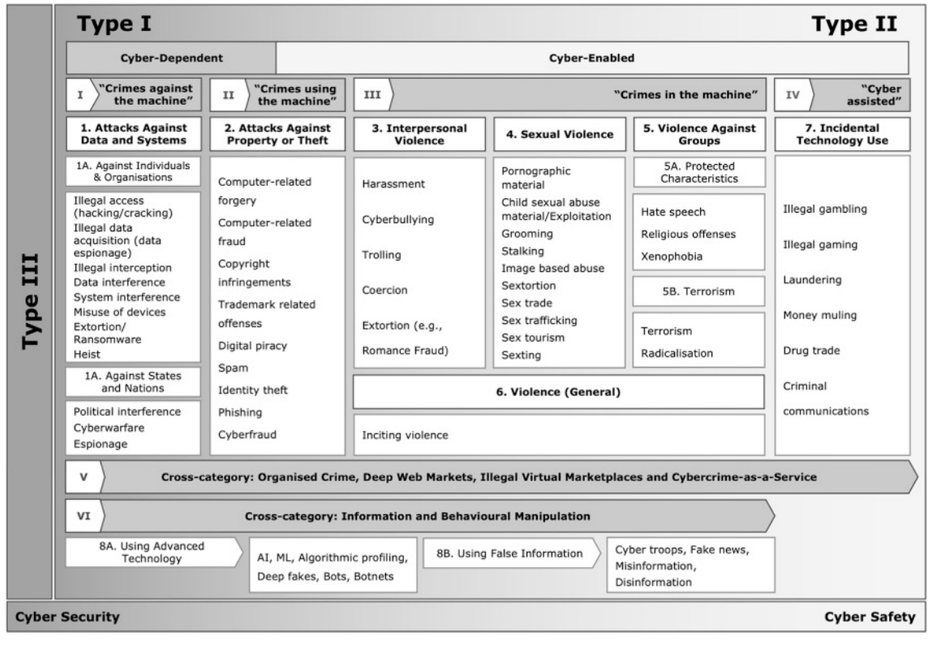

Abbildung 1: Cybercrime und Cyberdevianz, Klassifizierungsrahmen. Quelle: Forensic Sciences 2022, 2.

26 Vgl. Wall 2007.

2.2.2 Cybercrime-Definition des Bundeskriminalamtes

Laut Bundeskriminalamt (BKA) ist Cybercrime ein hochkomplexer, krimineller Wirtschaftszweig mit eigenen Wertschöpfungsketten und eines der sich am dynamischsten verändernden Kriminalitätsphänomene.[27] Um dieser Komplexität gerecht zu werden, setzen sich in Deutschland zunehmend die Begriffe Cybercrime oder Cyberkriminalität statt Computerkriminalität (so noch in der Budapest-Konvention) durch. Im Jahr 2020 verständigten sich das Bundeskriminalamt, welches jährlich ein Lagebild Cybercrime veröffentlicht, und die Verfasser*innen der Polizeilichen Kriminalstatistik (PKS) auf die Einführung eines neuen PKS-Summenschlüssels »Cybercrime« zur bundesweit einheitlichen Beschreibung dieser Straftaten. Er ersetzt seit 2021 den bis dato als »Computerkriminalität« ausgewiesenen Summenschlüssel.[28] Ähnlich den beiden oben dargestellten Kategorien »cyber-abhängig« und »cyber-gestützt« unterscheidet das Bundeskriminalamt zwischen »Cybercrime im engeren Sinne« (Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten) und »Cybercrime im weiteren Sinne« (Straftaten, die mittels Informationstechnik begangen werden). »Cybercrime im weiteren Sinne stellt also, vereinfacht gesagt, Taten dar, die auch in der analogen Welt begangen werden können, wie etwa der Drogenhandel. Cybercrime im engeren Sinne sind hochtechnische Straftaten, die ebensolche hochtechnische Ermittlungsarbeit aufseiten der Polizei erfordern. […] In der Underground Economy gibt es zahlreiche Marktplätze, auf denen illegale Güter wie Drogen, Waffen oder Kinderpornografie, gestohlene Daten und Identitäten, aber auch Dienstleistungen zur Begehung von Cyber-Straftaten angeboten werden – man spricht hierbei von Cybercrime-as-a-Service.«[29] Menschenhandelsdelikte sind allerdings nicht in der Cybercrime-Definition des BKA enthalten und finden damit auch keinen Eingang in das Lagebild Cybercrime.

2.2.3 Sexualisierte Gewalt im digitalen Umfeld/digitale Gewalt

Während es international nicht an unterschiedlichen Definitionen und Konzepten von Cybercrime mangelt, ist der Großteil dieser wissenschaftlichen, juristischen und kriminologischen Betrachtungen männlich dominiert. Daher fordern die Autor*innen in Forensic Sciences: »Angesichts der männlichen Dominanz im Bereich der Cyberkriminalität und der Cybersicherheit und der hohen Prävalenz geschlechtsspezifischer Online-Kriminalität mangelt es wohl an feministischen Ansätzen, um Cyberkriminalität zu definieren und zu erforschen. Künftige Beiträge auf diesem Gebiet sollten darauf abzielen, kriminologisch-feministische Beiträge und Perspektiven von Cybercrime anzuwenden, insbesondere auf Straftaten, die sich als sexualisierte Gewalt im Internet manifestieren.«[30]

Wie in den nachfolgenden Kapiteln noch detaillierter geschildert wird, bedienen sich Menschenhändler*innen Social-Media-Plattformen, um psychischen Druck auf die Betroffenen auszuüben. Dies geschieht sowohl während der Ausbeutungssituation, um die Betroffenen unter Kontrolle zu halten, als auch nach Beendigung der Ausbeutung, um eine Aussage der Betroffenen zu verhindern. Fachberatungsstellen berichten von Identitätsdiebstahl in Form von Fake-Accounts, also falschen Profilen, die im Namen der Betroffenen gegen ihren Willen oder ohne ihr Wissen angelegt werden, um Kontakt zu ihren Familien und ihrem sozialen Umfeld herzu-

27 BKA: Cybercrime. https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Cybercrime/cybercrime_node.html.
28 Vgl. BKA Bundeslagebild Cybercrime 2021.
29 BKA: Cybercrime. https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Cybercrime/cybercrime_node.html.
30 Forensic Sciences 2022, S. 395.

stellen. Häufig damit verbunden ist bildbasierte Gewalt, also die für die Betroffenen unfreiwillige Verbreitung intimer Aufnahmen.

Eine Studie des Europarates (2021),[31] die unter dem Blickwinkel des Gewaltschutzes von Frauen und Mädchen im digitalen Raum Bezüge zwischen der Istanbul-Konvention und der Cybercrime-Konvention erforscht, erfasst u. a. folgende Gewaltformen und Ausprägungen, von deren Vorkommen im Zusammenhang mit Fällen des Menschenhandels die Fachberatungsstellen in Deutschland ebenfalls berichten:

- Sexuelle Belästigung online: Dies kann das Versenden unerwünschter sexueller Bilder bedeuten, sexualisierte Kommentare, sexualisierte Diffamierung, sexualisierte Verleumdung
- Bilderbasierte sexuelle Belästigung: Sexuell suggestive oder private Fotos, die ohne Zustimmung aufgenommen und online geteilt wurden – sog. *Creepshots,* sexuelle oder private Bilder, die unter dem Rock oder Kleid ohne Einwilligung aufgenommen und online geteilt wurden – sog. *Upskirting*
- Bildgestützter sexueller Missbrauch: Nicht einvernehmliches Teilen von intimem Bild- oder Videomaterial, auch als webbasierte sexualisierte Gewalt bezeichnet (früher: *»Revenge Porn«*), *Deepfakes*, aufgezeichnete sexuelle Übergriffe und Vergewaltigungen, einschließlich sog. *Happy Slapping* (entweder live übertragen oder auf pornografischen Websites verbreitet)
- Bedrohungen und Nötigung, *Sexting, Sextortion,* Vergewaltigungsdrohungen, Anstiftung zur Vergewaltigung
- Formen von Online-Stalking, Überwachung oder Spionage in sozialen Medien oder Messaging-Diensten, Passwortdiebstahl, Spyware-Installation auf Geräten der Betroffenen, Tracking via GPS oder Geolocation.

In Deutschland setzte sich der Bundesverband Frauenberatungsstellen und Frauennotrufe e. V. (bff) als eine der ersten zivilgesellschaftlichen Organisationen mit dem Thema digitale Gewalt gegen Frauen auseinander. Bereits seit dem Jahr 2000 zeige sich eine Digitalisierung geschlechtsspezifischer Gewalt, wobei die Entwicklung in den letzten Jahren an Dynamik und Relevanz gewonnen habe: »Es findet gerade ein Umbruch statt, den noch niemand so vollumfänglich verstanden oder nachvollzogen hat« (Interview bff). Der bff definiert auf seiner Webseite[32] digitale Gewalt als: »[…] Sammelbegriff für verschiedene Formen geschlechtsspezifischer Gewalt. Gemeint sind Gewalthandlungen, die sich technischer Hilfsmittel und digitaler Medien (Handy, Apps, Internetanwendungen, Mails etc.) bedienen, und Gewalt, die im digitalen Raum, z. B. auf Online-Portalen oder sozialen Plattformen stattfindet. Wir gehen davon aus, dass digitale Gewalt nicht getrennt von ›analoger Gewalt‹ funktioniert, sondern meist eine Fortsetzung oder Ergänzung von Gewaltverhältnissen und -dynamiken darstellt.«

Besonderen Wert legt der bff auf einen angemessenen und nicht stigmatisierenden Sprachduktus, der die Perspektive der Betroffenen respektieren, das Strukturelle in Sprachdynamiken unterstreichen und das Problem digitaler sexualisierter Gewalt nicht individualisieren soll, »[…] denn es ist nicht individuell, sondern trennt sich an Geschlechtergrenzen« (Interview bff). An manchen

31 Council of Europe, 2021: Protecting women and girls from violence in the digital age. The relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in addressing online and technology-facilitated violence against women, S. 10.

32 bff: Aktiv gegen digitale Gewalt. https://www.frauen-gegen-gewalt.de/de/aktionen-themen/bff-aktiv-gegen-digitale-gewalt.html.

Stellen haben sich entsprechende alternative Begriffe bereits herauskristallisiert, beispielsweise bezüglich des sog. »Revenge Porn«, der stattdessen als »bildbasierte sexualisierte Gewalt« bezeichnet wird.

2.2.4 Psychische Gewalt im digitalen Umfeld

Die Trennlinie zwischen psychischem Druck und psychischer Gewalt scheint dünn, im analogen wie auch digitalen Kontext. Sämtliche oben aufgeführten digitalen Gewaltformen und Ausprägungen können als psychische Gewalt gelten. Die Istanbul-Konvention fasst darunter vorsätzliche Handlungen, die die psychische Integrität einer Person ernsthaft beeinträchtigen und schädigen. Das Übereinkommen definiert jedoch nicht, was unter einer solchen sog. ernsthaften Beeinträchtigung zu verstehen ist. Wie der erklärende Bericht zur Konvention ausführt, müssen die Elemente Zwang oder Androhung von Verhaltensweisen, die unter diese Bestimmung fallen, zur Anwendung kommen. Hervorzuheben ist, dass sich die Istanbul-Konvention hierbei nicht auf ein einzelnes Ereignis bezieht, sondern auf eine Vorgehensweise, die missbräuchliches Verhalten im Laufe der Zeit erfassen soll.[33]

Alle Formen von Gewalt gegen Frauen und Mädchen im digitalen Umfeld haben Auswirkungen auf die Psyche der Betroffenen und könnten daher als psychologische Gewalt eingestuft werden, die online und unter Einsatz von Informations- und Kommunikationstechnologien ausgeübt wird. Spezifische Merkmale digitalisierter Gewalt verstärken ihre Auswirkungen auf die Betroffenen, darunter fallen u. a. folgende Elemente:[34]

- Bereits das Erkennen digitaler Gewalt gestaltet sich schwierig, da die Grenzen zwischen Gewaltformen häufig verwischen und nicht immer klar strafrechtlich erfasst sind.
- Die meisten Formen digitaler Gewalt geschehen auf verschiedenen Plattformen, sowohl im öffentlichen als auch im privaten Bereich; Täter*innen können einen stärkeren Einfluss auf die Betroffenen ausüben, indem sie all diese Plattformen gleichzeitig bespielen. Eine Betroffene kann beispielsweise öffentlich mittels Social Media auf Instagram und Facebook diskreditiert werden und zur selben Zeit zusätzlich Droh-E-Mails erhalten, telefonisch belästigt werden oder auch auf offener Straße physisch von den Täter*innen eingeschüchtert werden.
- Typische Formen digitaler Gewalt beinhalten einen repetitiven Aspekt und eine Dauerhaftigkeit schädlicher Inhalte. So bergen die meisten Fälle von bildbasiertem Missbrauch das Potenzial, von Tausenden von Accounts überall im Internet geteilt zu werden und die Betroffenen endlos erneut zu viktimisieren.
- Die Beweislast liegt bei den Betroffenen, doch digitale Spuren können einfach gelöscht oder von Täter*innen verwischt werden; eine digitale Spurensicherung übersteigt oft die technischen Fähigkeiten der Betroffenen – und häufig auch die Fähigkeiten der Beraterinnen und der Polizei, wie in Kapitel 6 unter »Herausforderungen« näher erläutert wird –, oder die Betroffenen sind sich der Notwendigkeit, Spuren auch digitaler Gewalt zu sichern, gar nicht erst bewusst.

33 Council of Europe, 2011. Explanatory Report to the Council of Europe Convention on preventing and combating violence against women and domestic violence, Council of Europe Treaty Series No. 210.

34 Vgl. Council of Europe, 2021: Protecting women and girls from violence in the digital age. S. 11.

All diese Besonderheiten digitaler Gewalt verstärken ihre negativen Auswirkungen auf die Betroffenen und wirken sich in Konsequenz auch auf ihre Familien, Kinder und Beziehungen, auf ihre berufliche Situation, ihre Gesundheit und letztlich auf ihre Lebenserwartung aus. Eine EU-Studie veranschlagt die Gesamtkosten der Folgen von Cyber-Belästigung und Cyber-Stalking gegen Frauen auf 49 bis 89,3 Mrd. EUR pro Jahr. Darunter fallen Gesundheits- und Rechtskosten, Arbeitsmarktkosten und Kosten im Zusammenhang mit einer verminderten Lebensqualität.[35]

All diese Gewaltformen und Komponenten werden von den Fachberatungsstellen zunehmend in Fällen des Menschenhandels in Deutschland begleitend zur stattgefundenen Ausbeutung beobachtet.

3

MODUS OPERANDI IM DIGITALEN UMFELD

»Täter passen sich flexibel an technische und gesellschaftliche Entwicklungen an, agieren global und greifen dort an, wo es sich aus ihrer Sicht finanziell lohnt«, so das Bundeskriminalamt im Hinblick auf den Bereich Cybercrime generell.[36] Menschenhandel ist ein in erster Linie finanziell motiviertes Verbrechen. Es ist ein Geschäft, das wie jeder andere Markt auch auf Angebot und Nachfrage reagiert. Das Internet ist zum Hilfsmittel für die Tatdurchführung im Bereich des Menschenhandels geworden (Interview BKA), und Informations- und Kommunikationstechnologien haben das Geschäft für Menschenhändler*innen deutlich verbessert und vereinfacht.[37] Beispielsweise im Sinne einer enormen Ausweitung ihrer Möglichkeiten und Reichweite sowohl bzgl. der Suche neuer Opfer als auch für das Finden neuer Kundschaft. Menschenhändler*innen konkurrieren durchaus untereinander und versuchen, wie jedes Unternehmen auch, ihre Kosten gering zu halten. Hier vereinfachen IKTs ihr Geschäft, denn Menschenhändler*innen brauchen beispielsweise nun kein Bordell mehr zu betreiben. Damit entfallen Kosten für Miete, Strom, Sicherheit usw. Stattdessen können sie sexuelle Dienstleistungen online bewerben und lediglich ein Zimmer in einem Motel, Hotel, Airbnb o. Ä. mieten (Interview OSZE).

Bereits vor der Covid-19-Pandemie charakterisierte der Kriminologieprofessor Wall (2017) drei zentrale Aspekte von digitalen Netzwerktechnologien, die kriminelles Verhalten verändert haben.[38] Sie haben, erstens, einen »glokalisierenden« Effekt hervorgerufen durch ihren globalen Einfluss auf lokale Polizeidienste. So müsse sich beispielsweise die Fähigkeit der örtlichen Polizei zur Bekämpfung einer Straftat an neue Kriminalitätsformen, die in einem anderen Land verübt werden, anpassen. Zweitens können einzelne Täter*innen nun viele Individuen ortsunabhängig und gleichzeitig erreichen, Netzwerktechnologien haben also den Effekt einer asymmetrischen Beziehung. Dieser Effekt lässt sich beispielsweise in Cybergrooming-Fällen beobachten, in denen Täter*innen parallel viele Chats mit ihren potenziellen Opfern bedienen. Drittens kreieren Netzwerktechnologien und damit zusammenhängende Plattformen und soziale Medien neue Formen vernetzter und nicht-physischer sozialer Beziehungen, die als Quelle neuer krimineller Möglichkeiten dienen. Dies kann zum Beispiel in digitalem Stalking zum Ausdruck kommen oder in Sextortion, wenn Täter*innen Betroffenen damit drohen, deren private Nacktaufnahmen auf sozialen Plattformen zu verbreiten. Statt eine große, risikoreiche Straftat zu begehen, sei es nun ähnlich profitabel, viele kleine Verbrechen zu begehen, die ein deutlich geringeres Risiko der Aufdeckung für die Täter*innen bedeuten. Dies sei, vereinfacht gesagt, der Kern des kriminellen Nutzens digitaler Technologien.

Menschenhändler*innen nutzen das Internet und IKTs in jeder Phase des Ausbeutungsprozesses: 1) Zur Anwerbung neuer potenzieller Opfer, 2) für Transport und Logistik, 3) zur Kontrolle und Überwachung der Betroffenen.[39] Zusätzlich konnte in der Praxis der Fachberatungsstellen eine weitere kriminelle Nutzung von IKTs identifiziert werden, nämlich 4) zur Ausübung digitaler Gewalt nach Beendigung der Ausbeutungssituation, meist um eine Zeugenaussage der Betroffenen zu verhindern. Daher sollen die folgenden Abschnitte die Rolle von IKTs beim Modus Operandi der Täter*innen in allen vier Phasen erörtern und anhand von Fallbeispielen unterschiedliche Ausprägungen beleuchten. Der Einsatz von Technologie ist bisher nur für Menschenhandel zur sexuellen Ausbeutung als auch zur Arbeitsausbeutung bekannt, es gibt kaum verlässliche Hinweise auf eine mögliche Verbindung von IKTs mit anderen Ausbeutungsformen wie zum Beispiel der erzwungenen Betteltätigkeit.[40]

Während es im internationalen Kontext bereits etliche Aufsätze, Studien und Medienberichte zur Rolle sozialer Medien, IKTs und der Digitalisierung des Menschenhandels gibt,[41] scheint das Phänomen in Deutschland – ausgehend von der spärlichen Berichterstattung und lückenhaften Datenlage – noch relativ unerforscht und bisher eher durch anekdotische Fallbeispiele bekannt.

3.1 TECHNOLOGIEEINSATZ IN DER ANWERBUNG

Die Anwerbung potenzieller Opfer für Menschenhandel ist neben der tatsächlichen Ausbeutungssituation die Phase, in der Informations- und Kommunikationstechnologien die größte Rolle zu spielen scheinen, wie sowohl aktuelle Literatur[42] als auch das Bundeskriminalamt und Fachberatungsstellen bescheinigen. Social-Media-Plattformen wie Facebook, Instagram, TikTok, aber auch Messengerdienste wie Telegram und WhatsApp werden von Menschenhändler*innen genutzt, die damit im Vergleich zu analogen Anwerbemethoden wie Mund-zu-Mund-Propaganda oder Vermittlerbüros ihre Reichweite mit geringem Aufwand und Kosten enorm erweitern. Dabei gibt es nicht eine führende Plattform, die dafür genutzt wird, sondern alle interaktiven Kanäle, auf denen eine direkte Kontaktaufnahme möglich ist, gelten als sogenannte »enabler« und beherbergen das Potenzial für Ausbeutung (Interview BKA).

35 European Parliamentary Research Service, 2021: Combating gender-based violence: Cyber violence.

36 BKA: Was ist Cybercrime?

37 EUROPOL 2022: European Migrant Smuggling Center. 6th Annual Report.

38 Wall, D. S., 2017: Crime, security and information communication technologies: The changing cybersecurity threat landscape and implications for regulation and policing. In: Brownsword, R./Scotford, E./Yeung, K. (Hrsg.): The Oxford Handbook on the Law and Regulation of Technology, o. S.

39 Vgl. Raets, S./Janssens, J., 2019: Trafficking and Technology: Exploring the Role of Digital Communication Technologies in the Belgian Human Trafficking Business. In: European Journal on Criminal Policy and Research (2021) 27, S. 15–238; Vgl. EU-Strategie zur Bekämpfung des Menschenhandels 2021–2025.

40 Vgl. Council of Europe, 2022: Online and technology-facilitated trafficking in human beings; OSCE Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings, 2022: Policy Responses to Technology-Facilitated Trafficking in Human Beings: Analysis of Current Approaches and Considerations for Moving Forward.

41 Siehe beispielsweise Anti-Trafficking Review No. 14, 2020: Special Issue – Technology, Anti-Trafficking, and Speculative Futures.

42 Vgl. Council of Europe, 2022; Raets/Janssens, 2019; OSCE, 2022.

FALLBEISPIEL A

TEIL I – JADWIGA MÜNCHEN – LOVERBOY PER FACEBOOK-ANWERBUNG

A. wohnt mit ihren Eltern und dem jüngeren Bruder im ländlichen Raum Rumäniens. Die Familienverhältnisse sind prekär, Strom und fließend Wasser gibt es nur, wenn die Mutter einen Job ergattert, z. B. als Helferin in der Landwirtschaft. Der Vater ist alkoholkrank und arbeitslos, das Zusammenleben ist von häuslicher und sexualisierter Gewalt geprägt. Gegen den Willen des Vaters besuchen beide Kinder die Schule und absolvieren das Abitur, was jedoch andauernd zu Streit führt.

Nach dem Schulabschluss findet A. keine Arbeit und verbringt viel Zeit online, um sich von den Konflikten zu Hause abzulenken. Ein junger rumänischer Mann, der in Deutschland lebt, nimmt über Facebook Kontakt zu ihr auf. Sie chatten häufig, A. erzählt ihm von ihren Problemen mit den Eltern, der schwierigen wirtschaftlichen Lage der Familie, vom emotionalen Stress und dem Wunsch, ihren Bruder vor der Gewalt daheim zu schützen. Innerhalb weniger Wochen verliebt sich A. in den Mann, und sie fassen den Plan zu heiraten. Er bietet an, aus Deutschland zu kommen und sie daheim abzuholen, und verspricht ihr eine Arbeit als Managerin in Deutschland. Zu diesem Zeitpunkt ist A. 18 Jahre alt. Sie erzählt ihren Eltern nicht vom geplanten Umzug nach Deutschland, sondern gibt vor, lediglich in eine andere Stadt innerhalb Rumäniens umzuziehen. Ihr Vater droht damit, den Kontakt abzubrechen, sollte sie gehen.[43]

Die Kriterien, nach denen Menschenhändler*innen üblicherweise potenzielle Opfer zur sexuellen Ausbeutung auf Social Media identifizieren, drehen sich um Vulnerabilität, Zugänglichkeit und Attraktivität.[44] Das weitere Vorgehen zur Kontaktaufnahme und Erschleichung des Vertrauens erfordert schon größere Anstrengungen. Dabei können sich die Täter*innen zweierlei Strategien bedienen: Entweder sie »fischen« nach so vielen Opfern wie möglich, in der Hoffnung, jemand beißt an ihrem Köder an. Oder sie gehen gezielt vor und personalisieren den Cybergrooming-Prozess auf Basis eine Recherche öffentlich verfügbarer Daten des Opfers. Erleichtert wird eine solche personalisierte Ansprache durch die Tatsache, dass viele Menschen online eher bereit sind, Informationen über sich preiszugeben und für die Ansprache durch Fremde zugänglich sind. Täter*innen präsentieren sich online geschickt als das, wonach die potenziellen Opfer suchen, sowohl auf der emotional-zwischenmenschlichen Ebene als auch mittels Fake-Profilen, die von Wohlstand und einem hohen Lebensstandard zeugen.[45] Inzwischen ist in Fachkreisen der Aufbau einer vorgeblichen romantischen Beziehung mit der gleichzeitigen Kontrolle und sozialen Isolation der Betroffenen als Loverboy-Strategie bekannt.[46] Diese ebnet den Weg für »pseudo-intime und erotisierte Interaktionen«[47], in denen das Opfer Schritt für Schritt auf kommerzielle sexuelle

43 Siehe auch ARD-Dokumentation »Illegale Prostitution – Das gefährliche Geschäft mit dem Sex« vom 09.02.2022: https://www.ardmediathek.de/video/betrifft/illegale-prostitution-in-der-pandemie/swr/Y3JpZDovL3N3ci5kZS9hZXgvbzE2MTAxMzQ.

44 Vgl. Raets/Janssens, 2019.

45 Vgl. Council of Europe, 2022.

46 Siehe beispielsweise KOK-Rechtssprechungsdatenbank LG Aachen, Urteil vom 25.9.2019, Aktenzeichen 62 KLs 4/19. Schweren Menschenhandels nach der Loverboy-Methode, Kontaktanbahnung über Internetplattformen. https://www.kok-gegen-menschenhandel.de/rechtsprechungsdatenbank/datenbank/detailansicht?tx_t3ukudb_urteile%5Baction%5D=show&tx_t3ukudb_urteile%5Bcontroller%5D=Item&tx_t3ukudb_urteile%5Bitem%5D=385&cHash=eebac44fea7e8640008eae82c4c3642f.

47 Raets/Janssens 2019, S. 221, eigene Übersetzung.

Aktivitäten durch eine scheinbare Normalisierung solcher vorbereitet wird. Ermittlungen bulgarischer Behörden zeigen, »dass die Täter, bevor sie sich ihren potenziellen Opfern nähern und mit der Rekrutierung beginnen, die Fotos ihrer Opfer sorgfältig prüfen, um ihre Lebensumstände, ihren sozialen Status und ihr Umfeld, ihre familiären Beziehungen und ihren Beziehungsstatus wie Heirat, Scheidung oder Verlobung zu untersuchen. […] Erst nach einer solch sorgfältigen Untersuchung kontaktieren die Täter ihre Opfer und setzen dabei bemerkenswerte psychologische Fähigkeiten ein, um die Opfer zu überzeugen und zu motivieren, bestimmte Verhaltensweisen zu begehen.«[48]

FALLBEISPIEL B

FIZ – TIKTOK-ANWERBUNG UND AUSBEUTUNG ONLINE

Als B., eine 15-jährige Schülerin aus Dresden, nach den Lockdown-bedingten Schulschließungen wieder den Präsenzunterricht besucht, fällt den Lehrkräften auf, dass sie jeden Tag zu bestimmten Uhrzeiten auf ihr Smartphone fokussiert ist und sich aus dem Unterricht zurückzieht. Es stellt sich heraus, dass B. über TikTok einen älteren Mann aus Ostfriesland kennengelernt hatte, der ihr romantisches Interesse und eine Beziehung vortäuschte. Früh in ihrem Kontakt musste sie ihm erotische Bilder von sich schicken. Mehrmals täglich trafen sie sich zunächst auf TikTok und wechselten von dort in einen geschützten digitalen Raum, in dem sie ohne Moderation oder sonstige Meldemöglichkeiten allein waren. Er gab Instruktionen, welche sexuellen Handlungen sie an sich vornehmen sollte, von denen er Fotos und Videos machte und im Internet verkaufte. Aktuell laufen vier Gerichtsverfahren an vier unterschiedlichen Tatorten gegen den Tatverdächtigen, FIZ ist der Betroffenen zur Psychosozialen Prozessbegleitung beigeordnet.

In den letzten Jahren wurde eine zunehmende Kontaktanbahnung über das Internet auch in polizeilichen Statistiken des Bundeskriminalamtes vermerkt (Bundeslagebild Menschenhandel 2019, 2020). Im Jahr 2021 erfolgte in 55 Fällen (13,1 %) die Kontaktanbahnung über das Internet, wobei Betroffene sowohl über Social Media als auch über Inserate auf Online-Anzeigenportalen angeworben wurden.[49] Das Bundeskriminalamt vermutet einen Zusammenhang dieses Anstiegs mit dem pandemiebedingten Verbot der Prostitution, da Tatverdächtige für den Erwerb sexueller Dienstleistungen auf Social-Media- und Dating-Plattformen im Internet auswichen. Dass Täter*innen dabei häufig Pseudonyme bzw. Fake-Accounts verwenden, erschwere die polizeiliche Ermittlungsarbeit. »Zugleich dürfte das täterseitig eingeschätzte Risiko, bei der Begehung von Straftaten im digitalen Raum entdeckt zu werden, geringer sein.«[50]

Technologien erlauben es Menschenhändler*innen, unmittelbar auf sich neu präsentierende Gelegenheiten zu reagieren. So berichten Fachberatungsstellen, dass sich Menschenhändler*innen seit Kriegsbeginn in der Ukraine im Februar 2022 sowohl in bestehende Diasporagruppen für Menschen aus der Ukraine auf Internetplattformen wie Facebook als auch in Notfallgruppen bewegen, um Frauen für sexuelle oder Arbeitsausbeutung zu rekrutieren. Die für die Studie interviewten Fachberatungsstellen berichten gleichzeitig von einer proaktiven Internetrecherche osteuropäischer Frauen, wenn sie die Entscheidung treffen, zwecks Ausübung der Prostitution

48 Council of Europe 2022, S. 32, eigene Übersetzung.

49 BKA Bundeslagebild Menschenhandel 2021.

50 BKA Bundeslagebild Menschenhandel 2020, S. 24.

nach Deutschland zu gehen. Sie kontaktieren dann Bordelle über Social Media, führen Gehaltsverhandlungen darüber und bekommen relevante Informationen wie eine Kostenkalkulation der Lebenserhaltungskosten und Fotos des Zimmers auf ihr Smartphone geschickt. Der Transport wird häufig ebenfalls vom Bordellbesitzer organisiert, der einen Minivan zur Abholung der Frauen an ihren Heimatadressen schickt. Hier besteht eine große Sicherheitslücke, denn die Bekanntgabe des Wohnortes und womöglich ein Einblick in die Familienverhältnisse der Frau können im weiteren Verlauf der Ausbeutungssituation vom Bordellbesitzer als Druckmittel gegen sie verwendet werden.

3.2 ANWERBUNG FÜR ARBEITSAUSBEUTUNG

Anwerbung per Social Media und Internet findet nicht nur zur sexuellen Ausbeutung statt, sondern ebenso für Menschenhandel zur Ausbeutung der Arbeitskraft. Nach Angaben deutscher Behörden spielen Internet und Social Media auch in diesem Bereich eine zunehmend wichtige Rolle – wahrscheinlich zum Teil durch Covid-19 beschleunigt, da sich während der Lockdowns reelle Interaktionen ins Internet verlagern mussten.[51] Täter*innen inserieren zunächst auf verschiedenen Internetportalen ein Jobangebot, das trotz nicht geforderter beruflicher Qualifizierung oft vielversprechend klingt, aber dennoch möglichst vage gehalten ist.[52] Die Arbeitsplätze werden als gut bezahlt dargestellt, mit angeblich geregelten Arbeitszeiten. Nach ihrer Ankunft in Deutschland erhalten die Arbeitskräfte jedoch weder einen offiziellen Arbeitsvertrag noch einen Lohn oder nur einen Bruchteil der versprochenen Vergütung.[53]

Menschenhändler*innen inserieren nicht nur auf klassischen Job-Webseiten, sondern benutzen für ihre Zwecke auch spezielle Gruppen, in denen Menschen Arbeit in Deutschland suchen, z. B. »Bulgaren im Ausland« oder »*Nguoi tim viec*« (vietnamesisch für »Arbeitssuchende«).[54] Fachberatungsstellen und Bundeskriminalamt nennen daneben den Messengerdienst Telegram als relevantes Medium für die Rekrutierung zur Arbeitsausbeutung insbesondere in Osteuropa.[55] Das Internet hat Annoncen in der Zeitung und das Vermittlungsbüro ersetzt. Durch die Verlagerung der Rekrutierung in den digitalen Raum steigt das Risiko, auf Lockangebote hereinzufallen. Ohne analoges Vermittlungsbüro gestaltet sich die Anwerbungsphase deutlich kürzer, der Kontakt ist schneller und anonymer. Als besonders anfällig für Menschenhandel stufen die deutschen Behörden folgende Arbeitsfelder ein: Saisonarbeit in der Landwirtschaft, Reinigungsdienste, Gaststätten, Baugewerbe, Lebensmittelindustrie, Verkehr, Nagel- und Massagesalons.

Verglichen mit Menschenhandel zum Zwecke der sexuellen Ausbeutung scheint der Einsatz von Technologien für die Anwerbung für Arbeitsausbeutung jedoch trotz aller krimineller Möglichkeiten weniger verbreitet zu sein. Eine mögliche Erklärung könnte darin liegen, dass Arbeitskräfte häufig aus benachteiligten Regionen rekrutiert werden, wo der Zugang zu modernen Technologien bei Weitem nicht garantiert ist. »Aus dieser Perspektive wird die Online-Rekrutierung im Bereich des Menschenhandels durch eine technologische Kluft zwischen Opfern und Tätern behindert.«[56]

51 Vgl. Council of Europe, 2022.

52 Vgl. Raets/Janssens, 2019.

53 Vgl. Council of Europe, 2022.

54 Vgl. ebd.

55 Vgl. OSCE, 2022.

56 Raets/Janssens 2019, S. 222.

3.3 TECHNOLOGIEGESTÜTZTER TRANSPORT UND LOGISTIK

Menschenhandel, vor allem grenzüberschreitend, ist ein Delikt, das Absprachen und Koordination zwischen mehreren Personen benötigt. Nicht ein*e Menschenhändler*in begleitet die Betroffenen auf dem gesamten Weg, sondern es gibt aufgeteilte Aufgaben und Rollen. Es gibt Recruiter*innen am Heimatort der Betroffenen; diejenigen, die Kontakt zu beispielsweise Madames oder anders genannten Ausbeuter*innen herstellen; diejenigen, die die Flucht organisieren oder die Betroffenen bei der Flucht begleiten; Täter*innen, die den Lohn einstecken und Menschenhändler*innen am Ort der Ausbeutung. Technologien vereinfachen das Management und die Organisation des Menschenhandels und können daher als »grundlegende Geschäftsressource«[57] betrachtet werden. Mithilfe digitaler Kommunikationstechnologien entfällt sogar die Notwendigkeit für die Täter*innen, physisch beim Transport der Betroffenen anwesend zu sein. Die durch IKTs vereinfachte Online-Anwerbung und schlankere Logistik könnten dazu führen, dass das Geschäft Menschenhandel zukünftig von mehr Einzeltäter*innen betrieben wird, ohne in größeren organisierten Strukturen operieren zu müssen.[58]

FALLBEISPIEL

BUNDESKRIMINALAMT – »CALLCENTER«-MENSCHENHANDEL – TRANSPORT UND LOGISTIK

Ein neuer Modus Operandi zeigt sich beispielhaft in einem Fall des Menschenhandels zur sexuellen Ausbeutung in der Prostitution, der über die französischen Behörden an das Bundeskriminalamt herangetragen worden ist. Täter*innengruppierungen warben in Bulgarien Frauen für vermeintlich geregelte Arbeit in Frankreich, Deutschland und Belgien an. Anders als im Großteil der bisher bekannten Menschenhandelsfälle erfolgten Transport und Anreise der Frauen in die Zielwohnungen von den Täter*innen dirigiert eigenständig, ohne dass sie zu irgendeinem Zeitpunkt jemand aus der Täter*innengruppierung oder andere Betroffene abgeholt, begleitet oder empfangen hätte. Sämtliche Informationen bekamen die Frauen digital übermittelt und speicherten sie auf ihren Smartphones: elektronische Bustickets für die Überfahrt, Google-Maps-Adressen, Google-Street-View-Bilder zur Orientierung, wie die Straßen und Gebäude aussehen, Fotos der Wohnungen und Codes für die elektronischen Türschlösser der Wohnungen. Nach Ankunft sollten sich die Frauen telefonisch bei den Täter*innen melden.

Die Kundenakquise erfolgte über sogenannte Manager*innen in Polen, Rumänien und Deutschland. Sie übermittelten den Frauen täglich telefonisch die jeweiligen Termine mit Uhrzeit und Namen des Freiers und kontrollierten danach ebenfalls telefonisch die Einnahmen. Die Bezahlung erfolgte entweder bar an die Frauen, die sie dann mit Western Union weiterschicken mussten, oder die Freier transferierten das Geld über Paypal direkt an die Täter*innen. Aufgrund der Signifikanz des Telefons in diesem Fall betitelten die ermittelnden Kriminalbeamt*innen ihn als »Callcenter«-Menschenhandel. Der Fall wurde im Rahmen polizeilicher Kontrollen im Bereich der illegalen Wohnungsprostitution aufgedeckt, da auffällig schien, dass ein und dieselbe Person mehrere Wohnungen angemietet

57 Ebd., S. 223.

58 Vgl. ebd.

hatte, bei Kontrollen jedoch nie jemand außer immer wieder denselben Frauen angetroffen wurde.

Ein ähnliches Vorgehen berichten auch die Behörden aus Bosnien und Herzegowina.[59] Von dort organisierte und dirigierte ein Menschenhandelsring die sexuelle Ausbeutung bosnischer Frauen in Deutschland und Österreich, ohne selbst das Land zu verlassen. Die Täter*innen kontrollierten die Online-Profile der Betroffenen und vereinbarten Termine mit Freiern.

Der »Callcenter«-Fall verdeutlicht auch die große Problematik der Unsichtbarmachung Betroffener. Ihre Isolation, beispielsweise in Terminwohnungen, macht sie quasi unsichtbar und unerreichbar für klassische Hilfsangebote wie aufsuchende Straßensozialarbeit der Fachberatungsstellen.

3.4 DIGITALE KONTROLLE, ÜBERWACHUNG UND BEDROHUNG WÄHREND DER AUSBEUTUNGSPHASE

Der Einsatz digitaler Technologien während der eigentlichen Ausbeutungsphase des Menschenhandels zeichnet sich insbesondere durch die Macht aus, die Täter*innen zur Kontrolle, Überwachung und Bedrohung der Betroffenen erlangen, um das Geschäft weiterzuführen und einen Ausstieg aus der Ausbeutungssituation zu verhindern. Prostitution hat sich, besonders in Zeiten von pandemiebedingten Lockdowns, von klassischen Bordellen hin zu privateren oder Online-Ausübungsorten verschoben.[60] Täter*innen bieten mal mehr, mal weniger offen die »Dienstleistungen« der Betroffenen über Social Media, Escort-Webseiten, Plattformen wie früher kaufmich.de, aber auch über allgemeine Verkaufsplattformen wie Ebay-Kleinanzeigen und Trödelanzeigen an. Die darauffolgenden Terminabsprachen zwischen Täter*innen und Freier laufen meist telefonisch ab.

KOK-Rechtsprechungsdatenbank – Kontrolle der Prostitutionsausübung per Smartphone in einem sog. »Chinabordell«[61]

Der Hauptangeklagte Z. hatte von 2011 bis 2015 in mehreren deutschen Städten zahlreiche Bordelle bzw. Terminwohnungen geführt. Die in den Betriebsstätten beschäftigten 40 chinesischen Frauen wurden über chinesische Internetseiten für eine Tätigkeit in der Prostitution angeworben und reisten mit gefälschten Touristenvisa nach Deutschland ein. Teilweise streckten die Zuhälter*innen die Kosten für die falschen Papiere und die Einreise vor, die dann in Deutschland durch Prostitution abgearbeitet werden sollten. Die angeworbenen Frauen schliefen an ihren Arbeitsstätten, durften diese nur mit Erlaubnis verlassen und wurden von den Zuhälter*innen mit Lebensmitteln versorgt.

Z. erzielte einen Gesamtumsatz von knapp 2 Millionen €. Die Betriebsstätten waren durchgängig – 24 Stunden an sieben Tagen – geöffnet. Die Frauen arbeiteten während der gesamten Öffnungszeiten. In den Terminwohnungen warteten sie auf telefonisch vereinbarte Termine und standen Freiern jederzeit zur Verfügung. Die Frauen mussten jeden einzelnen Freierkontakt nach entsprechender Vorgabe telefonisch oder per WeChat (vergleichbar WhatsApp) an die Zuhälter*innen melden, zum Teil übermittelten die Frauen ihnen abends ein Foto der von ihnen für den Arbeitstag gefertigten Aufstellung. Dabei waren jeweils mitzuteilen Uhrzeit und Dauer der Prostitutionsleistung sowie die Höhe des Umsatzes und der Name der Frau.

59 Vgl. Council of Europe, 2022, S. 29.

60 Vgl. Teschner, G.: Sex on Demand. Prostitution geht online, Menschenhandel und Ausbeutung auch? In: Kriminalistik 11/2021, S. 645–648.

61 KOK-Rechtsprechungsdatenbank: LG Kleve vom 21.2.2017, Aktenzeichen 190 KLs-203 Js 98/15-2/16. https://www.kok-gegen-menschenhandel.de/rechtsprechungsdatenbank/datenbank/detailansicht?tx_t3ukudb_urteile%5Baction%5D=show&tx_t3ukudb_urteile%5Bcontroller%5D=Item&tx_t3ukudb_urteile%5Bitem%5D=274&cHash=9c2a405e13a891876c89fb7588fd51c3.

Informations- und Kommunikationstechnologien ermöglichen den Täter*innen eine räumliche Trennung zwischen sich und dem Ort der Ausbeutungshandlung und der Betroffenen, indem z. B. Betroffene Nachweise über die vollbrachte »Dienstleistung« online an die Täter*innen übermitteln muss. Auch eine physische Überwachung der Betroffenen entfällt durch digitale Technologien. Zypriotische, schweizerische und österreichische Behörden haben einen zunehmenden Einsatz von Apps zur Überwachung Betroffener von Menschenhandel vermerkt. Beispiele umfassen automatisierte Benachrichtigungen an die Mobiltelefone der Täter*innen, sobald die Betroffenen eine bestimmte Handlung wie das Öffnen der Wohnungstür tätigen. Täter*innen nutzen auch sog. Tracking-Apps zur Ermittlung des genauen Standortes, die sie – häufig ohne Wissen der Betroffenen – auf deren Smartphones installieren.[62] Tracking-Apps gehören in die übergeordnete Kategorie sog. Spyware, also Software oder Apps, die zur Ausspionierung von jemandem eingesetzt wird. Technisch einfach zu verstehen und preislich günstig zu erwerben, ermöglicht Spyware den Täter*innen, die betroffene Person »[…] direkt zu kontrollieren oder zu belästigen oder in das Handy des Opfers einzudringen und es zu überwachen. So erhält der Täter Zugriff auf die Kommunikation und den Aufenthaltsort des Opfers, einschließlich Browserverlauf, SMS, E-Mails, Anrufe, soziale Netzwerke, Medien wie Videos und Fotos, Passwörter einschließlich Bankkontopasswörter und deren Echtzeit-GPS-Ortung«.[63]

FALLBEISPIEL A, TEIL II

JADWIGA MÜNCHEN – LOVERBOY PER FACEBOOK-BEDROHUNG

Dem Plan folgend setzt A. ihr Vorhaben durch. Nach wenigen Tagen in München eröffnet ihr ihr Verlobter, sie müsse anschaffen gehen. A. ist schockiert und weigert sich anfänglich, doch ihr Unwille wird durch psychologische und körperliche Gewalt gebrochen. Er droht u. a. , sie aus dem Fenster zu werfen, ihren Eltern über Social Media Nacktaufnahmen von A. zu schicken und ihrer Familie etwas anzutun, deren Wohnort ihm bekannt ist, da er A. von zu Hause in Rumänien abgeholt hat. Er organisiert die Prostitution in München, wo sich A. im Kreisverwaltungsreferat als Sexworkerin registrieren muss. Die Angestellten dort erkennen Indikatoren von Zwang und rufen die Fachberatungsstelle Jadwiga an.

Kontrollausübung der Täter*innen über die Betroffenen funktioniert neben dem Einsatz technologischer Hilfsmittel auch über Bedrohung und Ausübung von Druck mithilfe von Social-Media-Kanälen. Fachberatungsstellen zufolge ist dies inzwischen Standard, insbesondere bei Fällen, in denen die Anwerbung online stattgefunden hat. Wenn Betroffene sich im Laufe des Ausbeutungsgeschehens zur Wehr setzen oder gar aufhören möchten, setzen Täter*innen das Internet

62 Europol, 2020: The challenges of countering human trafficking in the digital era.

63 Council of Europe, 2021, S. 33, eigene Übersetzung.

als Drohmittel ein. »Ich stelle deine Fotos online, ich sage deiner Familie, was du tust« (Interview FBS) sind gängige Taktiken, um den Willen Betroffener zu beugen. Daneben reglementieren Täter*innen die Internetnutzung ihrer Opfer oder übernehmen sogar die Bedienung ihrer Social-Media-Profile, um sie noch weiter von ihrem sozialen Umfeld zu isolieren.[64]

FALLBEISPIEL FIZ STUTTGART, TEIL I

SEXUELLE AUSBEUTUNG EINER NIGERIANISCHEN ANALPHABETIN

J. wird aufgrund einer sexuellen Beziehung zu einer Frau in Nigeria inhaftiert. Ein Bekannter der Familie holt sie aus dem Gefängnis – wobei unbekannt ist, ob er sie freigekauft oder herausgeschmuggelt hat. Es stellt sich heraus, dass er als »einer, der dort was zu sagen hat« Menschenhändler ist. Aus dem Gefängnis bringt er J. in ein Hotel in Lagos, das sie die folgenden sechs Monate nicht mehr verlassen wird. Der Täter übt heftige Gewalt gegen J. aus, um sie »gefügig zu machen«. Jedes Mal wenn sie gehen will oder den Sex mit ihm verweigert, schlägt er sie zusammen. In dieser Zeit wird sie zweimal von ihm schwanger, auf beide Male folgt eine Zwangsabtreibung, die ebenfalls in den Hotelräumen durchgeführt wird. Der Täter hat vor, J. nach Europa in die Zwangsprostitution zu schicken, suggeriert ihr jedoch Hilfe und Unterstützung, u. a. durch die Aussicht, eine Schule zu besuchen und Arbeit dort zu finden. J. erfasst die Hintergründe nicht, dass sie in die Hände eines Menschenhändlers geraten ist, doch »sie hatte eigentlich auch keine andere Wahl. Angesichts ihrer Mittellosigkeit, Vorstrafe und sexuellen Orientierung, wo hätte sie denn auch hingehen sollen?«.

J. ist Analphabetin. Dennoch wird sie allein per Flugzeug auf die Reise nach Europa mit der Zieldestination Deutschland geschickt. Der Täter schickt ihr die Bordkarte per WhatsApp und lotst sie während des gesamten Weges telefonisch. Ihr wird eine Nummer mitgegeben, die sie nach Ankunft in Stuttgart anrufen soll. Der Täter gibt J. zudem genaue Anweisungen, wo und wie sie einen Asylantrag zu stellen hat. Nach Ankunft übernimmt der Zuhälter eines Stuttgarter Bordells die Kontrolle über J. Sie muss in unterschiedlichen Bordellen und Terminwohnungen arbeiten, bekommt wieder telefonisch Anweisungen, die Bezahlung von wieder jemand anderem am Stuttgarter Hauptbahnhof einkassieren zu lassen. J. hält zum nigerianischen Menschenhändler telefonisch Kontakt und bittet mehrere Male darum, aussteigen zu dürfen. So habe sie sich das Leben in Europa nicht vorgestellt. Als sie sich irgendwann weigert weiterzuarbeiten, wird ihre Familie in Nigeria bedroht und letztendlich ihr Bruder erschossen. Dies ist der Wendepunkt für J. Über eine Straßensozialarbeiterin von einer Beratungsstelle für Vertriebene und Folteropfer gelingt ihr der Ausstieg, sie bekommt therapeutische Hilfe und wird von dort an die Fachberatungsstelle FIZ weitervermittelt. J. wechselt ihre Mobilnummer und ist, ohne jegliche Social-Media-Profile, nicht mehr für die Tätergruppierung erreichbar. Da der Menschenhändler allerdings ein Bekannter der Familie ist, droht er ihrer Familie in Nigeria weitere Gewalt an.

64 Vgl. Raets/Janssens, 2019.

3.5 DIGITALE GEWALT NACH DER AUSBEUTUNG

FALLBEISPIEL A, TEIL III

JADWIGA MÜNCHEN – LOVERBOY PER FACEBOOK – PSYCHISCHE GEWALT NACH DER AUSBEUTUNG

Im Gespräch mit einer Beraterin von Jadwiga öffnet sich A. schnell, berichtet von ihrer Notlage und wird in eine sichere Unterkunft gebracht. Anfangs möchte sie keine Strafanzeige gegen den Mann stellen, den sie als ihren Verlobten bezeichnet. Obwohl A. ihre Handynummer nach zwei Tagen in der Unterkunft wechselt, macht der Mann über den Facebook-Messenger mit Drohungen weiter, und auch seine Mutter und Großmutter üben per Messenger Druck auf A. aus, zu ihm zurückzugehen. Als die Drohungen gegen A.s Familie in Rumänien heftiger werden, entscheidet sie sich doch für eine Strafanzeige. Noch am selben Tag wird der Mann verhaftet. Während des Strafverfahrens bleibt A. zunächst als Opferzeugin vor Ort in Deutschland. Später im Prozess, als sie zurück in Rumänien ein Studium beginnt und aufgrund von Covid-19 die Einreise nach Deutschland nicht erlaubt ist, sagt sie per Videovernehmung aus. Das Gericht verhängt gegen den Täter eine Freiheitsstrafe von drei Jahren und drei Monaten wegen versuchter sexueller Ausbeutung.

Wenn Betroffenen der Weg aus einer Ausbeutungssituation gelingt, ist das selbstredend geschäftsschädigend für die Menschenhändler*innen. Diese haben ein starkes Interesse daran, die Betroffenen von einer Aussage bei Strafverfolgungsbehörden abzuhalten. Dahingehende Druckausübung, z. B. durch telefonische Drohanrufe, ist keine neue Vorgehensweise. Auch das Posten von Nacktbildern auf Social Media wie Facebook oder lediglich die Androhung davon ist inzwischen gängige Praxis von Täter*innen, wie Fachberatungsstellen bestätigen. Was allerdings neu ist, ist die erhöhte Vulnerabilität und mangelnde Kontrolle über private Daten. Die parallele Präsenz Betroffener auf multiplen Social-Media-Plattformen erweitert den Handlungsspielraum für Täter*innen. »Unsere Klientinnen sind ja in der Regel junge Leute unter 30. Natürlich sind sie auch nach der Straftat noch online« (Interview FBS). Durch ihre hohe Erreichbarkeit, Konnektivität und Aktivität in sozialen Medien können Menschenhändler*innen somit viel einfacher sowohl Kontakt zu den Betroffenen halten als auch deren soziales Milieu erreichen. Während in Deutschland zu diesem Aspekt noch keine Statistiken vorliegen, zeigen Zahlen aus den Niederlanden und den USA, dass dies dort bei etwa jedem dritten Menschenhandelsfall Realität ist.[65] Die Tatsache, dass Betroffene durchgängig aktive Internetuser*innen sind, macht auch eine Anpassung der Schutzkonzepte und IKT-Verhaltensrichtlinien in Schutzunterkünften erforderlich (siehe Kapitel 8).

Fachberatungsstellen zufolge gehen Täter*innen inzwischen jedoch noch weiter in der Verletzung der Privatsphäre der Betroffenen im digitalen Raum. So legen Täter*innen Fake-Profile im Namen ihrer früheren Opfer an und kontaktieren darüber deren Familien. Dieser Identitätsdiebstahl verbunden mit psychischem Druck auf die Betroffenen stellt eine erneute Straftat in Konse-

65 Vgl. Council of Europe, 2022; Polaris, 2018: On-Ramps, Intersections, and Exit Routes: A Roadmap for Systems and Industries to Prevent and Disrupt Human Trafficking.

quenz des Menschenhandels dar, wird jedoch bisher von der Polizei sehr unterschiedlich gehandhabt (siehe Kapitel 6).

Es sei allerdings darauf hingewiesen, dass all diese Methoden eine Erweiterung und Ergänzung des Täter*innenhandelns sind, sie ersetzen nicht zwangsläufig das von jeher bekannte Vorgehen von Menschenhändler*innen. Eine Betroffene kann beispielsweise infolge digitaler Drohungen ihre Social-Media-Accounts löschen, aber dennoch weiterhin Drohanrufe erhalten, aus denen hervorgeht, dass die Täter*innen sie analog beobachtet haben, u. a. durch die Beschreibung, welche Kleidung sie an diesem Tag trug. »Was danach bleibt, ist die ständige Angst. Könnte die Drohung in die Tat umgesetzt werden? Wenn dann auch noch intime Aufnahmen online kursieren, nimmt dieser psychische Stress für die Klientinnen kein Ende« (Interview FBS).

3.6 LIVESTREAMING ERWACHSENER BETROFFENER ALS TREND

Recherchen für die vorliegende Studie konnten keine neuen, rein auf Technologie basierenden Ausprägungen des Menschenhandels identifizieren – bis auf das Livestreaming sexualisierter Gewalt an erwachsenen Betroffenen. Ein Phänomen, das bis dato in erster Linie bei sexualisierter Gewalt an Kindern bekannt ist. Fachberatungsstellen in Deutschland hatten bereits solche Fälle, in denen Frauen von Menschenhändler*innen gezwungen und instruiert wurden, vor laufender Webcam auf bestimmten Plattformen sexuelle Handlungen an sich selbst vorzunehmen. Kund*innen können die live übertragene Darbietung aufnehmen und als Sexvideo weiterverkaufen. Auch dem Bundeskriminalamt ist dieser neue Trend bekannt (Interview BKA). Webcam-Shows gehören heutzutage zum gängigen Angebot der Erwachsenenpornografie. Für Kund*innen ist es aber durch einen geschickten Bildausschnitt, Videofilter etc. nahezu unmöglich festzustellen, ob die performende Person vor der Webcam möglicherweise dazu gezwungen wird. Livestreaming mit Menschenhandelsbetroffenen wird als schnell wachsender Bereich auch von weiteren Ländern gemeldet, u. a. Zypern, Spanien, Finnland und den Niederlanden. In Irland wird die Verlagerung von klassischen Plattformen zu sog. »pay as you go«-Videochat-Apps wie Escortfans und Onlyfans beobachtet, die private oder öffentliche Video-Chaträume bieten. Zunehmend werden dafür aber auch Dating-Apps und Social Media als Kanäle genutzt, die nicht primär auf sexuelle Dienstleistungen ausgerichtet sind.[66]

66 Vgl. Council of Europe, 2022.

4

DIE BEDEUTUNG VON DARKNET UND KRYPTOWÄHRUNGEN IM MENSCHENHANDEL

Nicht selten fallen im Zusammenhang mit Menschenhandel die Begriffe Darknet und Kryptowährungen. Ein gängiger Mythos im öffentlichen Bewusstsein ist, dass das Darknet als generell krimineller Bereich ein wichtiger Umschlagplatz für Menschenhändler*innen sei, die ihre kriminellen Machenschaften mit Bitcoins abwickeln. Alle drei Annahmen sind falsch. Weder ist die Nutzung des Darknets per se illegal, noch gibt es verlässliche Hinweise darauf, dass Menschenhandel sich in relevantem Ausmaß im Darknet abspielt, und auch die Bedeutung von Kryptowährungen in der finanziellen Abwicklung des Menschenhandels ist noch gering. Um ein grobes Verständnis dieses Themenkomplexes zu schaffen, soll es daher zunächst darum gehen, das Darknet im generellen Kontext des Internets einzuordnen und seine Relevanz für den Bereich Menschenhandel abzustecken. Danach werden Kryptowährungen als (k)eine Bezahlform des Menschenhandels erklärt, und abschließend wird kurz auf Geldtransfer im Menschenhandel eingegangen.

4.1 CLEAR NET, DEEP WEB UND DARKNET[67]

Das World Wide Web ist sinnbildlich wie ein Eisberg aufgebaut (siehe Abbildung 2): Das Internet, wie es die meisten Menschen im Alltag nutzen, ähnelt nur der sichtbaren zehnprozentigen Spitze des Eisbergs und stellt damit lediglich einen kleinen Teil des gesamten World Wide Webs dar. Es wird als Clear Net, Visible Web oder Surface Web bezeichnet. Es beinhaltet all diejenigen Bereiche des Internets, die man per üblichen Browsern (Chrome, Firefox, Safari u. a.) und mittels der Nutzung einer Suchmaschine (Google, Bing, DuckDuckGo u. a.) oder direkt per URL in der Adresszeile aufrufen und ohne weitere Einschränkungen nutzen kann.

90 Prozent des gesamten World Wide Webs hingegen befinden sich unter der Wasseroberfläche und diese werden Deep Web genannt. Das Deep Web bezeichnet diejenigen Bereiche des Internets, die nicht für das Auffinden durch herkömmliche Suchmaschinen indiziert wurden. Es umfasst in der Regel spezifische themengebundene Datenbanken oder Webseiten, die meist aufgrund von Zugriffsbeschränkungen (Login, z. B. Online-Banking, Behörden, Universitäten) oder wirtschaftlichen Interessen (Onlineshops) außen vor gelassen werden. Um auf diese meist harmlosen, passwortgeschützten oder zahlungspflichtigen Inhalte zugreifen zu können, muss man nur wissen, wo sie zu finden sind. Der Einsatz besonderer Tools ist nicht nötig.

67 Die folgenden Ausführungen basieren auf Fuß, M., 2020: Forensische Linguistik – Sprachanalyse in Darknet-Foren zu sexuellem Missbrauch und Ausbeutung von Kindern. https://dpt-statisch.s3.eu-central-1.amazonaws.com/dpt-digital/dpt-25/medien/dateien/454/2020_Darknet_Sprachanalyse_ECPAT-kurz.pdf; Gdta.at: Was ist eigentlich das Darknet? https://www.gdata.at/ratgeber/was-ist-eigentlich-das-darknet.

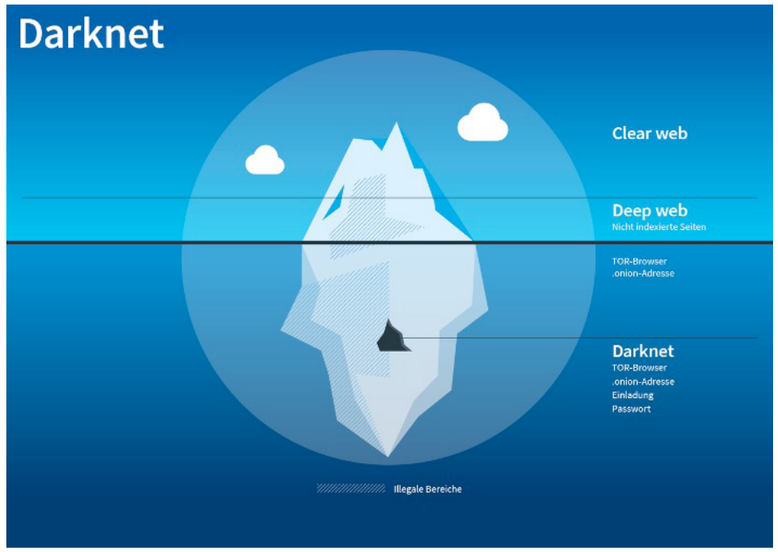

Abbildung 2: Illustrierung des Clear Webs, Deep Webs und Darknets. Quelle: Gdata.at – Was ist eigentlich das Darknet?

Das Darknet wiederum ist nur ein kleiner Teil des Deep Webs. Die Begriffe *Darknet oder Deep Web* werden häufig fälschlicherweise synonym verwendet, dabei sind sie keineswegs identisch. Das Deep Web funktioniert technisch wie das normale Clear Web über der Wasseroberfläche. Das Darknet hingegen kann man ohne verschlüsselten Zugang nicht betreten, denn es kommuniziert und funktioniert über ein eigenes Protokoll, das sog. Onion Routing.

4.2 TOR-NETZWERK

Onion Routing stellt keine direkte Verbindung zwischen zwei kommunizierenden Endgeräten (Computern) her, sondern durch eine Sequenz von Geräten, welche als Onion-Router bezeichnet werden. Jeder Onion-Router kann jeweils nur seinen Vorgänger und Nachfolger identifizieren, wodurch die Verbindung zwischen Sender*in und Empfänger*in anonym bleibt. Vereinfacht ausgedrückt: Der Datenverkehr wird über mehrere Server geleitet und bei jedem dieser Schritte verschlüsselt.

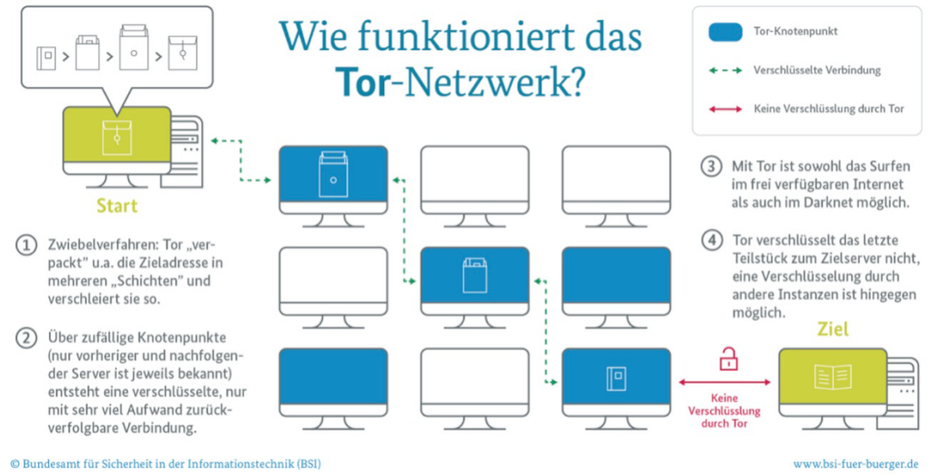

Abbildung 3: Wie funktioniert das TOR-Netzwerk? [68]

Zugang zum Darknet bekommt man nicht einfach über einen gewöhnlichen Browser. Es ist ein spezieller Browser nötig, welcher die Kommunikation mit dem Onion-Routing-Netzwerk erlaubt. Die bekannteste Verschlüsselung ist wohl der TOR-Browser, abgekürzt für The Onion Router (deutsch: Der Zwiebel-Router, als Hinweis auf die vielen Schichten wie die einer Zwiebel, welche die Daten durchdringen müssen). Dieser ist über die Homepage des TOR-Projekts[69] frei zugänglich. Ab diesem Zeitpunkt verhält sich der TOR-Browser auf den ersten Blick wie ein gängiger Browser, mit dem man wie gewohnt im Internet surfen kann.

Möchte man tatsächlich das Darknet erkunden, so ist für gewöhnlich der nächste Schritt das Ansurfen eines der vielen zur Verfügung stehenden sogenannten Hidden Wikis oder einer Darknet-spezifischen Suchmaschine. Bei Hidden Wikis handelt es sich um eine Art Katalog, der die unterschiedlichen Adressen des Darknets sammelt. Darknet-Adressen haben keine gewöhnliche namentliche Bezeichnung, wie beispielsweise Google als google.com, sondern stattdessen eine kaum einprägsame Zeichenfolge, welche stets auf ».onion« endet (Beispiel: 93hgh2vbia92gd-874hnaob.onion). Solche Adressen lassen sich ausschließlich über einen Browser ansurfen, der sich mit dem Onion-Routing-Netzwerk verbinden kann.

Das eigentliche Surfen im Darknet ist nicht per se illegal – es kommt nur darauf an, was man dort macht. Seit seiner Einführung Mitte der 90er-Jahre dient TOR auch Aktivist*innen, Oppositionellen und Journalist*innen als Plattform und Werkzeug, um Zensur in ihrem Heimatland zu umgehen, auf regional gesperrte Inhalte zuzugreifen und mit Gleichgesinnten anonymisiert zu kommunizieren, wie beispielsweise während der Protestbewegungen des Arabischen Frühlings[70]. Auch renommierte Nachrichtensender und Social-Media-Dienste bieten einen Onion-

68 Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Darknet-und-Deep-Web/darknet-und-deep-web_node.html

69 TOR-Projekt: https://www.torproject.org/de.

70 Bundeszentrale für politische Bildung: Der Arabische Frühling und seine Folgen.

Zugang zu ihren Webseiten an, darunter Deutsche Welle, BBC News, Twitter und Facebook.[71] Doch die Anonymität des Darknets bietet auch Kriminellen und Betrüger*innen Schutz und macht es zum beliebten Handelsplatz für illegale Geschäfte. Am häufigsten werden Dienstleistungen und Güter aus den folgenden Bereichen angeboten: illegale Drogen, Waffen, gefälschte Ausweispapiere und Visa, Auftragsmorde, Viren und Schadsoftware. Einer der größten Bereiche des Darknets bezieht sich auf sexualisierte Gewalt gegen Kinder und die Online-Darstellungen derselben, entweder durch einschlägige Foren mit Missbrauchsabbildungen, Angebote des Livestreamings sexualisierter Gewalt an Kindern oder das Anbieten von Kindern für sexualisierte Gewalt außerhalb des digitalen Umfelds.[72]

4.3 MENSCHENHANDEL IM DARKNET

Entgegen möglichen anderen Vermutungen spielt das Darknet bisher bei Menschenhandel keine signifikante Rolle, wie aktuelle Erkenntnisse zeigen.[73] Behält man den Fakt im Hinterkopf, dass Menschenhandel vor allem zur sexuellen Ausbeutung ein Geschäft basierend auf Angebot und Nachfrage ist und Menschenhändler*innen die größtmögliche Kundschaft zu erreichen suchen, scheint das Darknet in der Tat weniger dafür geeignet, genauso wenig wie für die Anwerbung potenzieller Opfer. Geht es jedoch um Nischenmärkte wie Organhandel, ist das Darknet durchaus als Umschlagplatz relevant.[74]

Auch die befragten Akteur*innen in Deutschland bestätigen diese Situation. Anders als bei Online-Missbrauchsabbildungen von Kindern verfügt das Bundeskriminalamt nicht über Erkenntnisse des Vorkommens von Menschenhandel zur sexuellen Ausbeutung im Darknet. Auch Fachberatungsstellen konnten bisher keine Fälle identifizieren, in denen Betroffene im Darknet angeboten oder ausgebeutet worden wären, wobei ein Unsicherheitsfaktor bleibt: »Wir können bestätigen, dass wir nichts von diesen Fällen wissen – nicht, dass das Darknet nicht relevant wäre.« »Wir sind da tatsächlich noch mehr im analogen Bereich unterwegs. Vielleicht wissen wir das [Anm.: den Einbezug des Darknets] nur nicht« (Interviews FBS). Fraglich ist allerdings, ob die Betroffenen selbst überhaupt wüssten, dass sich Täter*innen des Darknets als Werbeplattform für ihre Ausbeutung bedient haben.

4.4 KRYPTOWÄHRUNGEN, BITCOIN UND BLOCKCHAIN

Im Darknet erfolgen Zahlungen für illegale Dienste meist mit sogenannten Kryptowährungen, wovon Bitcoin die bekannteste ist. Kryptowährungen sind digitale Zahlungsmittel, die auf der sog. Blockchain-Technologie basieren. Blockchain-Technologie bietet die Möglichkeit, Daten in einem verteilten, dezentralen Netzwerk im Konsens zu verwalten. Dabei werden die Daten in Blöcken zusammengefasst und an eine stetig wachsende Kette gehängt, die sog. Blockchain. Kryptografische Mechanismen sorgen dafür, dass Dateien in der Blockchain nicht mehr verändert werden können und damit manipulationssicher sind.[75] Die direkte, schnelle und transparent nachvollziehbare Übertragung macht Kryptowährungen zu Zahlungssystemen ohne zentrale Instanz, was einen der größten Unterschiede zu traditionellen Finanzverwaltungen wie Banken darstellt.

71 Alec Muffet: Real World Onion Sites, 2022.

72 Kaspersky: Was ist das Darknet? https://www.kaspersky.de/resource-center/definitions/darknet; Council of Europe 2022.

73 Council of Europe 2022; Stop The Traffik, 2018: Human Trafficking and the Darknet: Insights on supply and demand.

74 OSCE 2020; Reid, R./Fox, B., 2020: Human Trafficking and the Darknet: Technology, Innovation, and Evolving Criminal Justice Strategies.

Guthaben wird in Form eines Computercodes zwischen zwei Teilnehmenden übertragen. Eine solche Übertragung wird durch eine kryptografisch signierte Transaktion in der Blockchain dokumentiert, wobei nur die Benutzer*innen- und Absender*innenadressen erfasst werden. Diese Adressen geben nicht die Identität des jeweiligen Bitcoins, der Nutzer*innen oder der Absender*innen an – sie identifizieren nur die jeweilige Transaktion. Nutzer*innen und Absender*innen sind mit einem sog. Wallet verknüpft. Wallets enthalten geheime Nummern (die ähnlich funktionieren wie Passwörter), die es Einzelpersonen ermöglichen, Bitcoins in den Wallets auszugeben.

Bitcoin ist als Open-Source-Währung konzipiert, die keiner Einzelperson, keinem Unternehmen und keiner Regierung gehört oder von diesen kontrolliert wird. Obwohl es technisch durchaus möglich ist, Nutzer*innen durch das Erkunden von Transaktionen auf einer Blockchain mit einer Adresse zu verknüpfen, gelten Bitcoins allgemeinhin als Währung, die schwierig zu verfolgen ist und damit Anonymität verspricht.[76] Diese Anonymität wird natürlich vor allem von denjenigen gesucht, die illegale Handlungen im Darknet begehen.

4.5 GELDTRANSFER IM MENSCHENHANDEL

Bezogen auf Menschenhandel scheinen Kryptowährungen weniger in Gebrauch zu sein als traditionelle Geldtransfermethoden wie Western Union oder MoneyGram.[77] Die scheinbare Unbeliebtheit von Kryptowährungen bei Menschenhändler*innen »[...] könnte auf die hohe Preisvolatilität und die Tatsache zurückzuführen sein, dass Kryptowährungen nur sporadisch als Zahlungsmittel akzeptiert werden, was das Einlösen virtuellen Geldes außerhalb des Systems recht unbequem macht. Mit anderen Worten scheint der größte Vorbehalt der durch Kryptowährungen unterstützten Geldwäsche zu sein, dass ›man zumindest ein gewisses Maß an Vertrauen in die gesamte Blockchain-Technologie haben muss‹. Als logische Folge davon werden technologische Fortschritte wie Bitcoin zwar den Menschenhandel erleichtern, aber nicht unbedingt sofort in den Modus Operandi des Menschenhandels integriert.«[78]

Das Bundeskriminalamt konnte mit Menschenhandel im Zusammenhang stehende Transaktionen mit Bitcoins bislang nur in Ausnahmesituationen feststellen. So kommt bei Delikten in Verbindung mit schwerer und organisierter Kriminalität wie Menschenhandel, Schleusung, Geldwäsche das sog. Hawala Banking System zur Anwendung, wie einzelne Ermittlungsverfahren belegen. Hawala beschreibt keine fest umrissene Methode des Geldtransfers, sondern umfasst

75 Bundesamt für Sicherheit in der Informationstechnik: Blockchain & Kryptowährung. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Technologien_sicher_gestalten/Blockchain-Kryptowaehrung/blockchain-kryptowaehrung_node.html.

76 Vgl. Reid/Fox, 2020.

77 Vgl. Council of Europe, 2022.

78 Raets/Janssens 2019, S. 225, eigene Übersetzung.

informelle, auf Vertrauen basierende Geldtransfersysteme.[79] Als während der Covid-19-Pandemie im Jahr 2020 internationale Reisen kaum mehr möglich waren und damit auch Hawala als Option wegfiel, erfolgten die Zahlungen in Fällen des nigerianischen Menschenhandels mit Bitcoins (Interview BKA).

Neueste internationale Erkenntnisse zeigen daneben den Einsatz von Messenger-Apps wie WeChat, um für Transaktionen im Zusammenhang mit Menschenhandelsfällen zu bezahlen, und weitere technologische Entwicklungen in diese Richtung sind denkbar.[80]

5

AKTUELLER RECHTSRAHMEN MIT RELEVANZ BEI TECHNOLOGIEGESTÜTZTEM MENSCHENHANDEL

5.1 INTERNATIONALER RECHTSRAHMEN

Aufholbedarf bei der EU-Richtlinie zur Bekämpfung des Menschenhandels

Die EU-Richtlinie 2011/36/EU vom 5. April 2011 zur Verhütung und Bekämpfung des Menschenhandels und zum Schutz seiner Opfer[81] ist ein grundlegend wichtiges Instrument bei den Bemühungen um die Bekämpfung des Menschenhandels in Deutschland und Europa. Ihre Umsetzung hat u. a. nationale Gesetzgebungen positiv beeinflusst, die Einführung von Koordinierungs- und Verweismechanismen für die Zusammenarbeit aller relevanter Akteur*innen hervorgebracht und grenzüberschreitende Zusammenarbeit befördert.[82] Trotz aller Fortschritte zeigt allerdings u. a. der Fortschrittsbericht[83] der Europäischen Kommission zur Überwachung der Umsetzung der Richtlinie, »[...] dass das zehn Jahre alte Instrument möglicherweise nicht mehr für den Zweck geeignet ist. Trotz der ergriffenen Präventionsinitiativen ist die Nachfrage nach den Diensten ausgebeuteter Opfer nicht zurückgegangen. In der EU besteht die Kultur der Straflosigkeit für Täter fort, und die Zahl der Strafverfolgungen und Verurteilungen von Menschenhändlern ist nach wie vor gering«[84]. Die wirtschaftlichen und sozialen Auswirkungen von

79 Deutscher Bundestag, Drucksache 19/16763, 19. Wahlperiode, 20.01.2020. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE. Drucksache 19/16101 – Nutzung des Hawala-Systems durch organisierte Kriminalität und terroristische Gruppierungen.

80 Vgl. Council of Europe, 2022.

81 RICHTLINIE 2011/36/EU DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 5. April 2011 zur Verhütung und Bekämpfung des Menschenhandels und zum Schutz seiner Opfer sowie zur Ersetzung des Rahmenbeschlusses 2002/629/JI des Rates.

82 EU-Fahrplan für die Umsetzung der Europäischen Strategie gegen Organisierte Kriminalität, Roadmap – Ares(2021)1264557.

83 BERICHT DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT. Dritter Bericht über die Fortschritte bei der Bekämpfung des Menschenhandels (2020) gemäß Artikel 20 der Richtlinie 2011/36/EU zur Verhütung und Bekämpfung des Menschenhandels und zum Schutz seiner Opfer, COM(2020) 661 final vom 20.10.2020.

84 EU-Strategie zur Bekämpfung des Menschenhandels 2021–2025.

Covid-19 haben die Situation weiter verschärft.[85] Unterstützungsangebote erreichen die Betroffenen nur noch schwer. Die Lage der Menschenhandelsbetroffenen habe sich nicht nur aktuell durch die Pandemie verschlechtert, sondern berge zusätzliche Gefahren durch die erwartete Rezession im Zuge der Pandemie.[86] Da die Mindestanforderungen für Schutz und Unterstützung der Betroffenen womöglich nicht mehr ausreichend sind, zieht die EU-Kommission die Konsequenz, auf Basis einer Evaluation der Richtlinienumsetzung eine »[...] Überarbeitung vorzuschlagen, damit die Richtlinie für ihre Zwecke geeignet ist«.[87] Die Reform wird voraussichtlich ab 2023 stattfinden.

EU-STRATEGIE ZUR BEKÄMPFUNG DES MENSCHENHANDELS 2021–2025 – Zusammenfassung und Einschätzung des KOK – Bundesweiter Koordinierungskreis gegen Menschenhandel e. V.[88]

Aus Sicht des KOK ist die EU-Richtlinie 2011/36 an vielen Stellen noch nicht ausreichend umgesetzt. In Deutschland wurden zwar die Regelungen zu weiteren Ausbeutungsformen durch die neuen strafrechtlichen Tatbestände umgesetzt, aber nicht die Bestimmungen zur Stärkung der Prävention und insbesondere des Opferschutzes unter Berücksichtigung der Geschlechterperspektive. Gerade die Umsetzung dieser Bestimmungen wäre allerdings wichtig für eine Veränderung der Situation von Betroffenen nicht nur in Deutschland. Die EU-Kommission erklärt in ihrer Strategie gegen Menschenhandel 2021–2025 zwar, dass sie die Mitgliedstaaten weiterhin bei der Umsetzung der Richtlinie unterstützt, u. a. durch gezielte Finanzierung, insbesondere im Hinblick auf geschlechtsspezifische und kindersensible Aspekte. Wünschenswert wäre an dieser Stelle aber insbesondere eine klarere Schwerpunktsetzung bei den Bestimmungen zu den Rechten der Betroffenen und zur Stärkung der Zivilgesellschaft in den Mitgliedstaaten.

Digitalisierung begegnen: Die Strategie der EU zur Bekämpfung des Menschenhandels 2021–2025 und zur Bekämpfung der organisierten Kriminalität 2021–2025

Ein zweiter zentraler Aspekt, den die EU-Kommission als Erklärung für die limitierte Wirksamkeit bestehender Rechtsinstrumente anführt, ist die Digitalisierung krimineller Aktivitäten, in der sich organisierte kriminelle Gruppen schneller an das sich verändernde soziale und wirtschaftliche Umfeld anpassen als Strafverfolgungsbehörden und Justiz: »Während es Straftätern gelingt, die neuesten Möglichkeiten des digitalen Zeitalters für ihre Zwecke zu nutzen, stehen die Strafverfolgungsbehörden vor großen Herausforderungen, mit den Entwicklungen Schritt zu halten. Dies umfasst die Erkennung von Anzeichen für Ausbeutung in der zunehmenden Menge

85 EU-Fahrplan für die Umsetzung der Europäischen Strategie gegen Organisierte Kriminalität, Roadmap – Ares(2021)1264557.

86 BERICHT DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT. Dritter Bericht über die Fortschritte bei der Bekämpfung des Menschenhandels (2020) gemäß Artikel 20 der Richtlinie 2011/36/EU zur Verhütung und Bekämpfung des Menschenhandels und zum Schutz seiner Opfer, COM(2020) 661 final vom 20.10.2020.

87 EU- Strategie zur Bekämpfung des Menschenhandels 2021–2025.

88 KOK, 02.06.2021. https://www.kok-gegen-menschenhandel.de/fileadmin/user_upload/images_web/_Kommentar_zur_neuen_EU-Strategie_zur_Bekaempfung_des_Menschenhandels__2021–2025__.pdf.

von Online-Anzeigen und die Beschaffung von wichtigen digitalen Beweisen.«[89] Beruhend auf dem rechtlichen und politischen Rahmen, den die EU-Richtlinie gegen Menschenhandel vorgibt, hat die EU-Kommission daher eine Strategie zur Bekämpfung des Menschenhandels 2021–2025 veröffentlicht.[90] Darin ist eines der Ziele die Zerschlagung des kriminellen Geschäftsmodells des Menschenhandels, online und offline. Besonderes Augenmerk legt die Strategie dabei auf die Online-Anwerbung, -Vermittlung, -Ausbeutung und -Bedrohung Minderjähriger, um eine Strafverfolgung all derjenigen zu erzielen, »[…] die Minderjährige zum Zwecke der Zwangskriminalität ausbeuten, die Opfern und ihren Familien gegenüber Gewalt anwenden oder sie damit bedrohen oder Opfer irreführen, indem sie vortäuschen, dass die Ausbeutung offiziell gemacht wird, die Opfer im Internet anwerben und dort Werbung für ihre Dienste machen und die auf Vermittler digitaler Dienste zurückgreifen«.[91]

Um die Zerschlagung des zunehmend digitalisierten Menschenhandelsmodells zu erreichen, setzt die Strategie einen Schwerpunkt auf den Aufbau von Kapazitäten durch systematische Schulungen von Strafverfolgungs- und Justizbehörden, u. a. zur Funktionsweise, Rolle und Nutzung von Technologien und sozialen Medien. Die Behörden sollen in eine Lage versetzt werden, in der sie »[…] zeitgemäß auf technologische Entwicklungen reagieren können«.[92] Einen weiteren Schwerpunkt legt die Strategie auf die verstärkte Zusammenarbeit von Strafverfolgungsbehörden und der Justiz bei grenzüberschreitenden und internationalen Fällen. Darüber hinaus ist zur Entlastung von Opferzeug*innen beabsichtigt, stärker als bisher elektronisches Beweismaterial im Strafverfahren zu berücksichtigen, sodass Gerichtsverfahren nicht mehr vorrangig von einer Aussage der Betroffenen abhängen. Dabei kann Europol verstärkt unterstützen, Internetinhalte aufzudecken, die Täter*innen nutzen. Eng damit verknüpft sind diejenigen in der EU-Strategie zur Bekämpfung der organisierten Kriminalität 2021–2025[93] definierten Maßnahmen, die, teils legislativer Natur, neben einer verbesserten Zusammenarbeit von Strafverfolgungsbehörden auch die Überwachung krimineller Finanzströme umfassen.

89 EU- Strategie zur Bekämpfung des Menschenhandels 2021–2025, S. 13.

90 MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN. Die Strategie der EU zur Bekämpfung des Menschenhandels, COM(2021) 171 final, 14.04.2021. https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52021DC0171&from=EN.

91 Schlussfolgerungen des Rates über die Festlegung der EU-Prioritäten für die Bekämpfung der schweren und organisierten Kriminalität im EMPACT-Zyklus 2022–2025, Brüssel, den 12. Mai 2021 (OR. en), 8665/21, S. 6. https://data.consilium.europa.eu/doc/document/ST-8665-2021-INIT/de/pdf.

92 EU- Strategie zur Bekämpfung des Menschenhandels 2021–2025, S. 13.

93 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über eine EU-Strategie zur Bekämpfung der organisierten Kriminalität 2021–2025, COM/2021/170 final.

EU-STRATEGIE ZUR BEKÄMPFUNG DES MENSCHENHANDELS 2021–2025 – Zusammenfassung und Einschätzung des Bundesweiten Koordinierungskreises gegen Menschenhandel – KOK e. V.[94]

Die EU-Strategie zielt ab auf eine verbesserte Erfassung und Übermittlung von Daten und Informationen bei der grenzüberschreitenden Strafverfolgung von Täter*innen. Unerwähnt bleiben dabei Datenschutzmaßnahmen, die aus Sicht des KOK jedoch immer Hand in Hand mit mehr Datenerfassung und -übermittlung gehen müssen. Denn diese Maßnahmen bergen großes Missbrauchspotenzial und könnten zulasten der Privatsphäre und des Schutzes der Betroffenen gehen. Mit Bezug auf die Datensicherung wäre auch das neuerliche Unterstreichen der Notwendigkeit der Einrichtung nationaler, eigenständiger Berichterstattungsstellen oder vergleichbarer Mechanismen wünschenswert gewesen, die durch die Menschenhandelsrichtlinie vorgesehen werden, aber von einigen Mitgliedstaaten, darunter Deutschland, noch nicht umgesetzt sind. Seit 2021 befindet sich die Einrichtung einer solchen Stelle am Deutschen Institut für Menschenrechte (DIMR) in einer Planungs- und Erprobungsphase. Voraussichtlich ab Ende 2022 soll die Stelle, angegliedert ans DIMR, die Arbeit aufnehmen.

E-Beweismittel: Zweites Zusatzprotokoll zur Cybercrime-Konvention

Wie in den vorhergehenden Kapiteln aufgezeigt, bedienen sich Täter*innen Social-Media-Plattformen und weiterer elektronischer Dienstanbieter für ihre kriminellen Machenschaften, u. a. um potenzielle Opfer anzuwerben, digitale psychische und bildbasierte Gewalt auszuüben oder um Missbrauchsabbildungen von Kindern zu verbreiten. Die Nutzung moderner Informations- und Kommunikationstechnologien durch Kriminelle beudeutet allerdings auch das Hinterlassen digitaler Spuren wie z. B. IP-Adressen, die für strafrechtliche Ermittlungsverfahren in Fällen des Menschenhandels große Relevanz haben können. Bisher gibt es nur die Cybercrime-Konvention des Europarats (sog. Budapest-Konvention, 2001), die als einziges völkerrechtliches Abkommen spezifisch auf die grenzüberschreitende Bekämpfung von Kriminalität im Internet abzielt (siehe Kapitel 2). Sie dient der Harmonisierung der Strafrechtsvorschriften im Bereich der Cyberkriminalität, der Bereitstellung von Strafverfahrensinstrumenten zur Verfolgung derjenigen Straftaten, die mithilfe eines Computersystems begangen werden, und der Förderung eines wirksamen Systems der internationalen Zusammenarbeit.[95] Der IKT-basierte Fortschritt macht es allerdings notwendig, rechtliche Lösungen für Herausforderungen zu finden, die es 2001 schlicht noch nicht gab. Laut EU-Kommission ist heutzutage mehr als die Hälfte aller strafrechtlichen Ermittlungen mit einem grenzüberschreitenden Antrag auf Zugang zu elektronischen Beweismitteln wie SMS, E-Mails oder Messaging-Apps verbunden.[96] Um auf diese Veränderungen besser zu reagieren, hat der Europarat nach vier Jahren Verhandlungen das Zusatzprotokoll zum Übereinkommen über Computerkriminalität betreffend die Verstärkung der

94 KOK, 02.06.2021. https://www.kok-gegen-menschenhandel.de/fileadmin/user_upload/images_web/_Kommentar_zur_neuen_EU-Strategie_zur_Bekaempfung_des_Menschenhandels__2021–2025__.pdf.

95 Vgl. Deutscher Bundestag, Kurzinformation: Die Budapest-Konvention (Cybercrime-Convention) – Aktueller Stand der Verhandlungen zum Zweiten Zusatzprotokoll des Europarates.

96 European Commission 2019: E-evidence – cross-border access to electronic evidence.

Zusammenarbeit und der Weitergabe von elektronischem Beweismaterial erarbeitet, das seit Mai 2022 offen für staatliche Unterzeichnungen ist.[97] Wie auch in den beiden oben dargestellten EU-Strategien stehen im Fokus des zweiten Zusatzprotokolls Maßnahmen zur Verbesserung der internationalen Zusammenarbeit der Strafverfolgungs- und Justizbehörden, Rechtshilfe zwischen Behörden sowie Zusammenarbeit und Informationsaustausch zwischen Behörden und privaten Dienstanbietern – auch mit Staaten außerhalb der EU – zur Gewinnung elektronischer Beweismittel. Da Beweismittel Dreh- und Angelpunkt jedes Strafverfahrens sind, ist die Befähigung der Strafverfolgungsbehörden, grenzüberschreitend Zugriff auf Daten als elektronische Beweismittel zu erlangen, die sich z. B. aus der Social-Media-Präsenz einer Person ergeben, ein wichtiger Schritt in der Bekämpfung von Cybercrime und damit auch bei Menschenhandelsfällen.[98] Das Zusatzprotokoll beinhaltet dabei gleichzeitig Garantien zum Schutz personenbezogener Daten sowie ein System von Menschenrechts- und Rechtsstaatlichkeitsgarantien.[99]

Online-Dienstanbieter und Plattformbetreiber in der Pflicht

Die Richtlinie über den elektronischen Geschäftsverkehr (*e-Commerce Directive*)[100] aus dem Jahr 2000 gilt als Eckpfeiler für die digitale Regulierung. Seit ihrem Inkrafttreten vor über 20 Jahren sind jedoch neue Möglichkeiten entstanden, mithilfe von Informations- und Kommunikationstechnologien Geschäfte zu tätigen und internetbasierte Dienste anzubieten. Dies brachte neben viel Fortschritt auch neue Herausforderungen und Risiken, die vom bisherigen Rechtsrahmen nicht erfasst worden sind. So waren Plattformbetreiber und Online-Dienstanbieter bisher kaum für die über sie laufenden Inhalte zur Rechenschaft zu ziehen, selbst wenn diese illegaler Natur waren. Dementsprechend sah es die Europäische Kommission als notwendig an, den Rechtsrahmen zu erweitern und neue Vorschriften zu erlassen, die das Internet zu einem sichereren Raum für Nutzer*innen in Europa machen. Im Dezember 2020 hat sie ein umfassendes Regulierungspaket bestehend aus dem Gesetz über digitale Dienste (*Digital Services Act – DSA*)[101] und dem Gesetz über digitale Märkte (*Digital Markets Act – DMA*)[102] vorgelegt. Letzteres schafft harmonisierte Verpflichtungen und Verbote für große systemrelevante digitale Plattformen mit erheblicher Marktmacht in der EU, sog. *Gatekeeper*, soll jedoch angesichts seiner bedingten Relevanz für die Thematik der vorliegenden Studie nicht weiter ausgeführt werden.

Der DSA trägt der Tatsache Rechnung, dass der digitale Raum nicht unreguliert und rechtsfrei werden bzw. bleiben darf. Im Vordergrund der neuen Regulierungen stehen der Schutz der Grundrechte von Nutzer*innen, die Bekämpfung illegaler Inhalte und Falschinformationen sowie die Schaffung eines einzigen, EU-einheitlichen und soliden Rahmens für die Transparenz und Rechenschaftspflicht der Online-Plattformen und elektronischen Anbieter. Anbieter elektronischer Dienste fungieren als Bindeglied zwischen Nutzer*innen und den angebotenen Waren, Dienstleistungen und Inhalten im digitalen Raum, deshalb sollen sie deutlich stärker als bisher in die Verantwortung genommen werden. Dies gilt sowohl für Online-Vermittler wie Internetdienstanbieter als auch für Betreiber von Cloud- und Messaging-Diensten, Marktplätzen oder sozialen Netzwerken. Für Hosting-Dienste und insbesondere für Online-Plattformen wie Social-Media-Netzwerke, Plattformen für das Teilen von Inhalten, App-Stores, Online-Marktplätze und Online-Reise- und Unterkunftsvermittlungs-Plattformen gelten besondere Sorgfaltspflichten. Die Bestimmungen stehen in einem angemessenen Verhältnis zu der Art der betreffenden Dienste und sind auf die Zahl der Nutzer*innen zugeschnitten. Sehr große Online-Plattformen und Suchmaschinen, die mindestens 45 Millionen Nutzer*innen in der EU bzw. 10 % der Bevölkerung erreichen, unterliegen strengeren Anforderungen als z. B. Start-ups. So müssen sie u. a. künftig eine Risikominderungsanalyse durchführen, die insbesondere auf Risiken wie digitale Gewalt gegen Frauen, Verbreitung illegaler Inhalte oder jugendgefährdende Inhalte eingeht. Alle Maßnahmen müssen dabei sorgfältig gegen Beschränkungen der Meinungsfreiheit abgewogen werden. Eine Beaufsichtigung in Form unabhängiger Prüfungen der Risikomanagementmaßnahmen ist vorgesehen.

Die neuen Vorschriften enthalten europaweite Bestimmungen für die Erkennung, Meldung und Entfernung illegaler Inhalte und zielen auch spezifisch auf den Schutz Minderjähriger auf allen Plattformen in der EU ab. Wenn ein Betreiber einer Online-Plattform beispielsweise von einer vergangenen, aktuellen oder geplanten schwerwiegenden Straftat Kenntnis bekommt, die eine Bedrohung für das Leben oder die Sicherheit einer Person bedeutet, muss er unverzüglich die Strafverfolgungs- oder Justizbehörden des betroffenen Mitgliedstaates informieren und alle relevanten Informationen zur Verfügung stellen. Darüber hinaus wird für alle Plattformbetreiber das sog. *notice and takedown*-Prinzip verpflichtend, um illegale oder rechtsverletzende Inhalte von ihren Plattformen nach deren Meldung (*notice*) innerhalb einer gesetzten Frist zu beseitigen (*takedown*), was z. B. für Betroffene von bildbasierter Gewalt eine bessere Handhabe bedeutet. Eine allgemeine Verpflichtung, die auf der Plattform übermittelten oder gespeicherten Informationen zu überwachen oder aktiv nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hindeuten, ist allerdings – wie auch schon in der Richtlinie über den elektronischen Geschäftsverkehr – weiterhin nicht vorgesehen.[103]

Das Europäische Parlament und der Rat erzielten am 23. April 2022 eine Einigung über die Vorschriften des DSA und des DMA.[104]

Das Gesetz über digitale Dienste steht in Kohärenz mit anderen europäischen Rechtsvorschriften, insbesondere dem Vorschlag zur Verbesserung des Schutzes von Kindern vor sexuellem Missbrauch (2022)[105], der wiederum im Einklang mit der EU-Strategie für eine wirksamere Bekämpfung des sexuellen Missbrauchs von Kindern (2020)[106] und der umfassenden

97 Zweites Zusatzprotokoll zum Übereinkommen über Computerkriminalität betreffend die Verstärkung der Zusammenarbeit und der Weitergabe von elektronischem Beweismaterial, 12.05.2022.

98 Council of Europe 2022, S. 92 f.

99 Vgl. Council of Europe – Cybercrime. https://www.coe.int/en/web/cybercrime/opening-for-signature-of-the-second-additional-protocol-to-the-cybercrime-convention.

100 Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt (»Richtlinie über den elektronischen Geschäftsverkehr«).

101 Legislative Entschließung des Europäischen Parlaments vom 5. Juli 2022 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über einen Binnenmarkt für digitale Dienste (Gesetz über digitale Dienste) und zur Änderung der Richtlinie 2000/31/EG (COM(2020)0825 – C9-0418/2020 – 2020/0361(COD)).

102 Legislative Entschließung des Europäischen Parlaments vom 5. Juli 2022 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über bestreitbare und faire Märkte im digitalen Sektor (Gesetz über digitale Märkte) (COM(2020)0842 – C9-0419/2020 – 2020/0374(COD)).

103 BVDW. Digital Services Act/Digital Markets Act; EU-Kommission, Pressemitteilung vom 23.04.2022. Gesetz über digitale Dienste: Kommission begrüßt politische Einigung über Vorschriften zur Gewährleistung eines sicheren und verantwortungsvollen Online-Umfelds.

104 Pressemitteilung, 05.07.2022. Paket zu digitalen Diensten: Kommission begrüßt Annahme des neuen EU-Regelwerks für digitale Dienste durch das Europäische Parlament.

105 Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern, COM(2022) 209 final 2022/0155(COD), 11.05.2022.

106 MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN – EU-Strategie für eine wirksamere Bekämpfung des sexuellen Missbrauchs von Kindern.

Kinderrechtsstrategie 2021–2024 der EU[107] steht. Konkret bedeutet dies eine Verpflichtung der Anbieter von Online-Diensten, bekannte Inhalte mit Missbrauchsabbildungen von Kindern oder diesbezügliche Handlungen aufzudecken und den Behörden zu melden. Für den Schutz Minderjähriger, die auf einschlägigen Webseiten zur sexuellen Ausbeutung angeboten werden, ist das durchaus relevant. Der Vorschlag beinhaltet jeodoch keine weiteren menschenhandelsspezifischen Vorschriften.

Gemäß der aktuellen EU-Strategie zur Bekämpfung des Menschenhandels wird die EU-Kommission über das Gesetz über digitale Dienste hinaus einen Dialog mit einschlägigen Internet- und Technologieunternehmen führen und ähnliche Dialoge auf nationaler Ebene unterstützen, um die Nutzung von Online-Plattformen für die Anwerbung und Ausbeutung von Betroffenen des Menschenhandels einzudämmen. »Die Zusammenarbeit mit dem privaten Sektor wird daher gefördert, um Innovationen und Fachwissen für die Entwicklung technologiebasierter Lösungen zur Unterstützung der Prävention und Bekämpfung des Menschenhandels zu nutzen. Präventions- und Aufklärungsmaßnahmen, unter anderem zur sicheren Nutzung des Internets und sozialer Medien, könnten weiter dazu beitragen, das Risiko des Kinderhandels zu mindern.«[108]

Unspezifische und auf Freiwilligkeit von Plattformbetreibern basierende Altersüberprüfung

Unklar ist zudem, wie die Altersverifikation auf Online-Plattformen konkret aussehen wird. Das Gesetz über digitale Dienste spricht von »gezielte[n] Maßnahmen zum Schutz der Rechte des Kindes, darunter auch Werkzeuge zur Altersüberprüfung und zur elterlichen Kontrolle sowie Werkzeuge, die es Minderjährigen ermöglichen sollen, Missbrauch zu melden bzw. Unterstützung zu erhalten« (Artikel 27). Dies wird von der EU-Strategie für ein besseres Internet für Kinder (2022, BIK+)[109] aufgegriffen, demnach die Kommission einen EU-Verhaltenskodex zur altersgerechten Gestaltung fördern wird, der auf den neuen Bestimmungen des DSA aufbauen und u. a. mit der Datenschutzgrundverordnung (DSGVO)[110] im Einklang stehen soll. Der Kodex soll darauf abzielen, die Privatsphäre und die Sicherheit von Kindern bei der Nutzung digitaler Produkte und Dienstleistungen zu gewährleisten. Die Teilnahme von Online-Plattformbetreibern an der Entwicklung und Umsetzung solcher Verhaltenskodizes ist jedoch freiwillig. Die EU-Kommission, so die BIK+ weiter, wird »[…] Methoden unterstützen, mit denen der Altersnachweis unter Wahrung der Privatsphäre und Sicherheit EU-weit anerkannt werden kann. Die Kommission wird vorrangig mit den Mitgliedstaaten (die im Einklang mit den nationalen Rechtsvorschriften die Möglichkeit haben, Personen unter 18 Jahren elektronische Ausweise auszustellen, im Rahmen des jüngsten Vorschlags für eine europäische digitale Identität), den relevanten Stakholdern und den europäischen Normungsorganisationen zusammenarbeiten, um wirksame Altersüberprüfungsmethoden zu stärken. Diese Arbeiten werden Marktlösungen durch einen robusten Zertifizierungs- und Interoperabilitätsrahmen fördern.«[111] Es bleibt abzuwarten, als wie erfolgreich sich dieses Vorhaben erweisen wird.

107 MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN – EU-Kinderrechtsstrategie, COM(2021) 142 final, 24.03.2021.

108 EU-Strategie gegen Menschenhandel 2021–2025, S. 11.

109 COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS – A digital decade for children and youth: the new European strategy for a better internet for kids (BIK+), COM(2022) 212 final, 11.5.2022.

110 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

5.2 EIN BLICK AUF DEN DEUTSCHEN RECHTSRAHMEN

Die ungenügende Inverantwortungnahme von Plattformbetreibern und fehlende oder unzureichende Altersüberprüfung wurden einhellig von allen für diese Studie befragten Fachleuten als zwei fundamentale Lücken kritisiert. »Du bist ein Unternehmen. Was tust du, um sicherzustellen, dass Kinder nicht deinetwegen vergewaltigt werden? Was tun diese Webseiten, um Kinder zu schützen?« (Interview OSZE). Selbst auf digitalen Marktplätzen wie kaufmich.de und weiteren Plattformen, die vom Bundeskriminalamt als sog. *high risk enabler* festgestellt wurden, gibt es keine verpflichtenden Alterskontrollen. »Das müsste geändert werden« (Interview BKA). Als problematisch nennt das BKA in diesem Zusammenhang sog. Taschengeldtreffen, bei denen Jugendliche selbstinitiativ sexuelle Darstellungen und Dienstleistungen gegen Geld im Internet anbieten.[112] Dies erfolgt nicht nur über einschlägige Seiten, sondern auch über herkömmliche Dienstleistungsplattformen wie markt.de. Eine gesetzliche Nachsteuerung sieht das Bundeskriminalamt als angebracht.

Bis auf die eben erwähnten Punkte konnten die befragten Akteur*innen für ihre Arbeit keine Gesetzeslücken des deutschen Strafgesetzbuchs benennen, die unter Berücksichtigung technologischer Komponenten des Verbrechens eine Strafverfolgung von Menschenhandelsfällen und damit zusammenhängenden Delikten verhindern oder erschweren würden. Bisher scheint auch die Unterstützung der Betroffenen in diesem Kontext ausreichend von den aktuellen rechtlichen Regelungen abgedeckt zu sein, vorbehaltlich der schon lange bekannten Gesetzeslücken, deren Korrektur der KOK seit vielen Jahren fordert.[113] Die Tatmittel, die im Straftatbestand beschrieben sind, decken auch die digitalen Komponenten des Menschenhandels ab, zudem spielt das Tatmittel Internet bei bisherigen Menschenhandelsermittlungen eine untergeordnete Rolle, da damit zusammenhängende Taten nach wie vor in der Mehrzahl analog sind und daher auch analoge Ermittlungen erfordern (Interview BKA). Aus Sicht von Strafverfolgung und Justiz sollten Gesetze nicht zu detailliert auf spezifische IKTs ausgerichtet sein, »[…] damit man ein Auslegungsmoment und die Möglichkeit hat, neue Technologien darunter zu fassen« (Interview Staatsanwaltschaft Berlin). Ein solcher technologieneutraler Rechtsrahmen ist auch die Empfehlung des UN-Kinderrechteausschusses bezüglich Straftaten mittels neuer Technologien, da die Erwähnung spezifischer technologischer Programme oder Instrumente im Gesetz kontraproduktiv sein kann. Rechtsvorschriften sollen so umfassend wie möglich definiert werden und deutlich zum Ausdruck bringen, dass alle technischen Mittel, die in irgendeiner Weise zur Begehung von sexualisierter Gewalt und Ausbeutung von Kindern eingesetzt werden, unter das nationale Recht fallen.[114]

111 BIK+ 2022, S. 10, eigene Übersetzung.

112 Siehe BKA Bundeslagebericht Menschenhandel 2020.

113 Siehe KOK-Forderungskatalog zur Bundestagswahl 2021.

114 Vgl. ECPAT International, 2019: Explanatory Report to the Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography.

Cyberstalking: Anpassung an den technischen Fortschritt in § 238 Strafgesetzbuch

Positiv hervorzuheben ist, dass der Gesetzgeber in Deutschland eine Änderung des Strafgesetzbuches (StGB) zur besseren Erfassung von Cyberstalking in § 238 StGB »Nachstellung«[115] vorgenommen hat, die 2021 in Kraft getreten ist. Der Anpassungsbedarf wurde mit dem technischen Fortschritt und der damit einhergehenden Zunahme des Cyberstalkings begründet: »Über sogenannte Stalking-Apps beziehungsweise Stalkingware können Täter auch ohne vertiefte IT-Kenntnisse unbefugt auf E-Mail- oder Social-Media-Konten sowie Bewegungsdaten von Opfern zugreifen und so deren Sozialleben ausspähen. Cyberstalking erfolgt aber nicht nur durch den unbefugten Zugriff auf Daten des Opfers, sondern insbesondere auch dadurch, dass Täter unter Vortäuschung der Identität eines Opfers etwa in sozialen Medien Konten anlegen und unter dem Namen des Opfers abträgliche Erklärungen abgeben oder Fotos von ihm veröffentlichen. Diese besonderen Begehungsweisen von Nachstellungstaten gilt es gesetzlich besser und rechtssicherer zu erfassen.«[116] Praktikerinnen aus Beratungsstellen bleiben eher vorsichtig optimistisch bei dieser Neufassung des Cyberstalking-Paragrafen. Vergleiche man es mit der Reform des Sexualstrafrechts 2016, durch die sich in den letzten fünf Jahren leider an der tatsächlichen Situation für Frauen nicht viel verbessert habe, werde eine Gesetzesreform allein kaum Erfolg haben, wenn sie nicht von unterstützenden Maßnahmen wie Fortbildungen für die Justiz und Entwicklung digitaler Ermittlungskapazitäten der Polizei flankiert werden.[117]

6

HERAUSFORDERUNGEN UND HÜRDEN

Es liegt wohl in der kriminellen Natur der Sache, dass die Bemühungen zur Verhinderung und Beseitigung des Menschenhandels und zur Unterstützung der Betroffenen dem Phänomen an sich immer mindestens einen Schritt hinterherhinken. Wie eine Fachberatungsstelle es zusammenfasste: »Täter haben den Vorteil, dass sie nicht legal arbeiten und daher ganz andere Grenzen überschreiten und Dinge ausprobieren können. Sie haben den Vorsprung, dass sie sich nur damit beschäftigen können, wie sie besser an ihr Ziel kommen« (Interview FBS). Die schnellen Entwicklungen im Menschenhandel, die der Fortschritt der Informations- und Kommunikationstechnologien mit sich brachte, stellen Staaten vor neue und drängende Herausforderungen. Die UN mahnen, dass »[…] der zukünftige Erfolg bei der Beseitigung des Menschenhandels in seinen

115 § 238 StGB: https://www.gesetze-im-internet.de/stgb/__238.html.

116 Bundesministerium der Justiz, Gesetzgebungsverfahren, 17. August 2021. Gesetz zur Änderung des Strafgesetzbuches – effektivere Bekämpfung von Nachstellungen und bessere Erfassung des Cyberstalkings.

117 bff-Interview. Für eine ausführliche Auseinandersetzung des bff mit der Neufassung des § 238 StGB siehe: Stellungnahme zum Referentenentwurf eines Gesetzes zur Änderung des Strafgesetzbuches – effektivere Bekämpfung von Nachstellungen und bessere Erfassung des Cyberstalkings, 2021. https://www.frauen-gegen-gewalt.de/de/stellungnahmen-1718/stellungnahme-zum-referentenentwurf-eines-gesetzes-zur-änderung-des-strafgesetzbuches-effektivere-bekämpfung-von-nachstellungen.html. Zum Gesetz zur Verbesserung des Schutzes der sexuellen Selbstbestimmung siehe: https://www.bundesregierung.de/breg-de/aktuelles/mehr-schutz-vor-sexueller-gewalt-393682; eine kritische Zwischenbilanz ist nachzulesen unter: https://www.deutschlandfunkkultur.de/reform-des-sexualstrafrechts-bilanz-nach-fuenf-jahren-100.html.

vielfältigen Formen […] davon [abhängt], wie Staaten und Gesellschaften darauf vorbereitet und dafür gerüstet sind, Technologien in ihren Antworten zu nutzen«. [118]

Gleichzeitig ist zu beachten, dass Informations- und Kommunikationstechnologien sich in stetiger und schneller Entwicklung befinden, und damit auch Cyberkriminalität. Während Staaten teilweise erst damit beginnen, zielgerichtet und strukturiert Kapazitäten für digitale Ermittlungen im Clear Web aufzubauen, gibt es beispielsweise schon erste Berichte über sexualisierte Gewalt im Metaverse.[119] Typologisierungen wie die hier in Kapitel 2 vorgestellte sind hilfreich bei der Erfassung aufkommender Phänomene, können jedoch nicht deren gesamte Komplexität erfassen, sondern reduzieren sie auf eine Handvoll Kategorien und beispielhafte Straftatausprägungen. Sie sind auch aufgrund ihrer scharfen Abgrenzungen problematisch, wie die Autor*innen von Abbildung 1 selbst anerkennen und auf die Möglichkeit verweisen, zukünftige Cybercrime-Klassifizierungen weniger voneinander abgetrennt, sondern als Spektrum mit fließenden Übergängen zu denken und/oder basierend auf der Motivation und Absicht der Täter*innen.[120] Vor dem Hintergrund der neuen Normalität im Bereich Cybercrime bedarf es Klassifizierungen, die sowohl die aktuelle Realität in ihrer Komplexität abbilden als auch Flexibilität weiterer Entwicklungen zulassen. Fortgeschrittene Technologien wie Künstliche Intelligenz, Virtuelle Realität oder Deep Fakes bei der Ausübung neuer Straftaten sind bisher kaum in den aktuellen Schemata berücksichtigt und bedürfen weiterer Forschung.

Hürden bei Strafverfolgungs- und Justizbehörden aus EU-Perspektive

Neue Anforderungen für Strafverfolgungs- und Justizbehörden ergeben sich vor allem in zwei Bereichen. Zum einen benötigen sie auf nationaler Ebene die entsprechenden technischen Fähigkeiten, um auf technologische Herausforderungen und den digitalen Modus Operandi der Menschenhändler*innen zu reagieren. Zum anderen muss die Interoperabilität der Systeme gegeben sein, um auch außerhalb des eigenen Zuständigkeitsbereichs zusammenarbeiten zu können.

Laut EU-Kommission weisen mehr als 80 % der heutigen Straftaten eine digitale Komponente auf, und selbst bei Offline-Straftaten müsste »fast jeder Strafverfolgungsbeamte und Staatsanwalt die Grundlagen kennen, um Straftaten online zu ermitteln«.[121] Es bestehe ein dringender Bedarf, die Kapazitäten und Fähigkeiten der nicht spezialisierten Strafverfolgungsbehörden und Staatsanwaltschaften zu erhöhen. Sie müssen mit den Fähigkeiten, Fertigkeiten und dem Wissen über verfügbare Instrumente, Dienstleistungen und Technologien Schritt halten und

118 Inter-Agency Coordination Group against Trafficking of Persons (ICAT). Human Trafficking and Technology: Trends, Challenges and Opportunities. Issue Brief 7/2019.

119 Bracket Foundation, 2022: Gaming and the Metaverse. The Alarming Rise of Online Sexual Exploitation and Abuse of Children Within the New Digital Frontier; Definition Metaverse: »Das Metaverse […] ist ein virtueller Raum, in dem sich Benutzer mit Hilfe von Avataren bewegen und in dem sie virtuelle Artefakte beeinflussen und nutzen können, etwa wenn sie sich Kleidung überziehen, ein Haus bauen und dieses einrichten, eine Tür öffnen und auf die Straße hinaustreten und dort Mitspieler und Gleichgesinnte treffen. Wie in der realen Welt kann man dort leben, arbeiten, lernen, Handel treiben, Gespräche führen und Beziehungen aufbauen. Der Begriff ist aus »Meta–« (»auf einer höheren Stufe stehend«, »auf einer anderen Ebene angesiedelt«) und »Universe« (»Universum«) zusammengefügt. Je nach Perspektive und Manifestation ist ein Metaverse eine Ausprägung der virtuellen Realität (Virtual Reality) oder auch der Mixed Reality, wenn Elemente der Realität wie auf Text und Ton basierende Konversation und am Körper erfahrene Sexualität wesentlich sind.« (Gabler Wirtschaftslexikon. https://wirtschaftslexikon.gabler.de/definition/metaverse-123520).

120 Vgl. Forensic Sciences, 2022-2, S. 393 ff.

121 EU-Strategie gegen Menschenhandel 2021–2025, S. 31.

brauchen operatives Know-how, so die EU-Kommission weiter.[122] Darüber hinaus fehlt es an Fachwissen über Ermittlungen in speziellen Bereichen wie der digitalen Forensik von Geräten und Daten ebenso wie in der Nutzung von Open-Source-Lösungen, weil die Behörden »[…] nicht wissen, welche Lösungen entwickelt wurden und verfügbar sind, weil die Anforderungen und das Fachwissen unterschiedlich sind und weil es an Unterstützung für die Weiterentwicklung und Wartung mangelt«.[123]

Die Folgen dieser Unzulänglichkeiten sind drastisch: Das Sekretariat der Budapest-Konvention geht davon aus, dass nur ein Prozent aller Cyber-Straftaten überhaupt an die Strafverfolgungsbehörden gemeldet werde, und von diesen Meldungen führe weniger als ein Prozent zu einem Ergebnis innerhalb des Justizsystems.[124] Im BKA-Lagebild Cybercrime 2021 lag die Aufklärungsquote mit knapp unter 30 % weiterhin deutlich unter dem PKS-Durchschnitt.[125]

Schon vor der Digitalisierung des Modus Operandi von Menschenhändlern erforderten Fälle oft eine internationale Zusammenarbeit zwischen Behörden, Institutionen und weiteren Akteuren, da kriminelle Netzwerke häufig auch grenzüberschreitend agieren. Die dafür notwendigen Strukturen bei Strafverfolgung und Justiz scheinen auch viele Jahre, nachdem es alle menschenhandelsrelevanten Instrumente fordern, noch immer aufgrund mangelnder Ressourcen, Koordination und Kommunikation nicht stabil genug, um auf die stetig wachsenden Anforderungen von Online-Ermittlungen adäquat reagieren zu können. Zwar unterstützen EU-Agenturen wie Europol und Eurojust sowohl bei der angestimmten Entwicklung von Kompetenzen als auch bei der koordinierten Zusammenarbeit zwischen den nationalen Behörden, doch um digitalisierten Menschenhandel aufzudecken und zu verfolgen, müssen Informationssysteme untereinander kompatibel sein, gemäß aktueller EU-Strategie gegen Menschenhandel.

Herausforderungen und Hürden in Deutschland

Die aktuell 42 im KOK organisierten spezialisierten Fachberatungsstellen für Betroffene des Menschenhandels in Deutschland, der Schweiz und Südtirol leisten unentbehrliche Arbeit für die Verwirklichung der Rechte von Betroffenen und füllen nicht selten dort die Lücke, wo staatliche Strukturen fehlen. Ihre Expertise baut auf jahrzehntelanger Praxis im Umgang mit Klient*innen und der Zusammenarbeit mit Polizei und Politik auf. Doch die Digitalisierung des Menschenhandels stellt auch Fachberatungsstellen vor Herausforderungen. Durchaus selbstkritisch identifizieren sie bestimmte Schwierigkeiten, ihre eigenen Arbeitsweisen den digitalen Entwicklungen anzupassen, als auch Hürden in Hinblick auf weitere gesellschaftliche Sphären, die für die Arbeit gegen Menschenhandel relevant sind. Diese Beobachtungen wurden um Informationen von Strafverfolgung und Justiz erweitert und zeigen im Folgenden die wichtigsten daraus identifizierten Lücken und Hindernisse in Deutschland auf.

122 Siehe Mitteilung der Kommission »Gewährleistung der EU-weiten Rechtspflege – Eine Strategie für die justizielle Aus- und Fortbildung auf europäischer Ebene für den Zeitraum 2021–2024«, COM(2020) 713 final vom 2.12.2020. Darin wird die Notwendigkeit hervorgehoben, Fachkräfte zur Bewältigung neuer Herausforderungen zu befähigen.

123 EU-Strategie gegen Menschenhandel 2021–2025, S. 31.

124 Vgl. Council of Europe, 2021, S. 12.

125 Vgl. BKA Bundeslagebild Cybercrime 2021.

Verständnis der Thematik und Entwicklung neuer Ansätze stehen am Anfang

»Ich glaube, in Deutschland ist das alles noch zu sehr am Anfang. Du merkst ja, selbst wir, die mit dem Thema zu tun haben, haben auch nicht so viel Durchblick, was das Thema angeht. Ich glaube, das muss einfach stärker nach vorne gebracht werden.« »Wir sind da verhältnismäßig blank. Zu Online- und digitalen Aspekten des Menschenhandels wissen wir zu wenig.« Diese beiden Aussagen von Fachberatungsstellen stehen sinnbildlich für die Situation der Praktiker*innen von deutschen Beratungsstellen als auch der Polizei, wie sie aus Erfahrungen der FBS eingeschätzt wird. Während FBS neue Trends und Ausprägungen des Menschenhandels in der Regel schnell wahrnehmen und darauf reagieren, z. B. durch die Erweiterung ihrer Angebote für spezielle Zielgruppen wie Frauen und Kindern auf der Flucht, wurden die technologiegestützten Einflüsse auf den Menschenhandel bisher oft in der Gesamtbreite der Themen, die Fachberatungsstellen abdecken, unterschätzt oder als Sonderthema betrachtet. »Bis vor Kurzem dachte ich, es reicht, wenn zwei Mitarbeiterinnen auf eine Fortbildung gehen und sich damit [dem technologiegestützten Menschenhandel] auskennen. Aber ich glaube, das ist falsch gedacht. Wir müssen es als Querschnittsthema denken, das alle [Beraterinnen] brauchen, weil es überall mit reinspielt« (Interview FBS).

Mangelndes gesellschaftliches und behördliches Bewusstsein für digitale Gewalt

Formen digitaler psychologischer und sexualisierter Gewalt sind relativ neue Phänomene, die Überschneidungen aufweisen und häufig noch keine klaren Rechtsdefinitionen haben.[126] Während manche dieser Gewaltformen schon in Medien und damit allgemeiner im gesellschaftlichen Bewusstsein angekommen zu sein scheinen, mangelt es an Verständnis für andere. Der bff veranschaulicht das am Beispiel Hate Speech als eine der bekannteren Formen digitaler Gewalt im Kontrast zu Online-Stalking: »Bei Partnerschaftsgewalt und sexualisierter Gewalt haben wir eine größere gesellschaftliche Tabuisierung als bei Hate Speech. Bei Hate Speech fällt es den meisten Leuten leicht zu verstehen, dass es falsch ist, wenn z. B. eine Journalistin oder Wissenschaftlerin dafür bedroht wird, dass sie ihren Job macht. Aber sobald es darum geht, dass ein verletzter Ex-Freund seiner Ex-Partnerin nachstellt, fällt es vielen Leuten schwerer sich mit der Betroffenen zu solidarisieren, sondern dann wird das Täterverhalten entschuldigt« (Interview bff).

Bezogen auf Menschenhandelsfälle, in denen Täter*innen online psychischen Druck auf die Betroffenen ausüben, beklagen Fachberatungsstellen in der Zusammenarbeit mit der Polizei bisher mangelnde Sensibilität der Behörden. Die Bedrohung werde nicht immer ernst genommen, und eine gängige Antwort auf den Versuch, Online-Druck zur Anzeige zu bringen, sei eine Version von: »Schalt halt das Handy aus, was ist das denn für ein Problem? Der [Täter] ist doch gar nicht da, der kann dir doch gar nichts tun.« Diese Schwierigkeiten werden auch in einem Bericht des Europarats (2021) genannt: »Bei Online- und technologiegestützter Gewalt gegen Frauen ist es in vielen Ländern eine Herausforderung, von ausgebildeten Strafverfolgungsbeamten gehört und ernst genommen zu werden. […] Die meisten Strafverfolgungsbeamten sind nicht ausgebildet, um die verschiedenen Formen von Gewalt gegen Frauen und Mädchen im Internet zu erkennen, und viele von ihnen wissen nicht, wie sie damit umgehen sollen. Diese mangelnde Ausbildung beeinträchtigt die Fähigkeit der Frauen, Beschwerden wirksam einzureichen.«[127] Oder, wie eine FBS es auf den Punkt bringt: »Im Moment ist es leider Glückssache, wo die Betroffenen hingeraten« (Interview FBS).

126 Vgl. Council of Europe, 2021, S. 11.

127 Council of Europe, 2021, S. 11, eigene Übersetzung.

Schwierigkeiten mit Beweislast und digitaler Beweissicherung

Werden Betroffene nach der Ausbeutung weiterhin von Täter*innen bedroht und möchten dies zur Anzeige bei der Polizei bringen, zeigt die Praxis bisher, dass die Hinweise oft nicht für einen Tatanfangsverdacht ausreichen. Wenn die Menschenhändler*innen keine klaren Drohungen vornehmen, wie z. B. physisch vor der Tür zu stehen, sondern die Betroffenen »nur« online über Fake-Profile unter Druck setzen, kann die Polizei häufig einen solchen Online-Tatanfangsverdacht nicht konkret auf die Menschenhändler*innen als Täter*innen zurückführen. Die Beweislast liegt bei den Betroffenen selbst, die sich dessen jedoch nicht immer bewusst sind und es versäumen, digitale Beweise z. B. mittels Screenshots zu sichern, bevor diese von den Täter*innen wieder gelöscht werden. Zumal ist nicht jede*r Betroffene dafür technologieaffin genug. Hierbei können sie selten auf kompetente Unterstützung durch Fachberatungsstellen bauen: »Ich weiß ja gar nicht, was man bräuchte vonseiten der Strafverfolgung. Was bleibt zum Beispiel übrig im digitalen Raum, wenn man die Accounts löscht?« (Interview FBS).

Die Sicherung digitaler Beweise durch die Betroffenen in akuten Ausbeutungssituationen bedarf nicht nur Wissen darüber, sondern auch einer gewissen Geistesgegenwärtigkeit. Es gibt durchaus Fälle, in denen betroffene Frauen mit ihren Smartphones z. B. Fotos von Ortschaften und Straßennamen gemacht und bei sich behalten haben, was im Strafverfahren hilfreich und relevant war. Doch Fachberatungsstellen berichten von einer verschärften Problematik der digitalen Beweislast bei Betroffenen mit wenig Bildung oder gar Analphabet*innen, die weniger geübt im Umgang mit Informations- und Kommunikationstechnologien sind. »Je weniger gebildet eine Frau ist, desto gefährlicher ist es für sie, denn desto schlechter sind später die Beweise und ihre Glaubhaftigkeit im Strafverfahren. Es bleibt alles vage« (Interview FBS). Vor Gericht liegt der Knackpunkt darin, eine Zwangslage der Betroffenen nachzuweisen trotz vornehmlicher Online-Methoden der Menschenhändler*innen, wie beispielsweise im sog. Callcenter-Fallbeispiel in Kapitel 3. »Bei Menschenhandel passiert der Zwang häufig auf persönlicher Ebene hinter verschlossenen Türen, wo der Täter auf die Frau einwirkt. Das passiert in den seltensten Fällen über WhatsApp oder per Sprachnachricht. Daher bin ich auf den Personalbeweis, also die Aussage der Geschädigten angewiesen. Wir sind schon dazu übergegangen, viel mehr Telekommunikationsüberwachung zu machen, uns auch Chats anzugucken und Telefonate abzuhören. Das Problem ist aber, die Täter reden natürlich nicht am Telefon darüber«, ist die Erfahrung der spezialisierten Menschenhandels-Staatsanwaltschaft Berlin. Daher seien Telekommunikationsdaten in der Regel zwar als Indiz nutzbar, können allein aber nicht als Nachweise für Zwangslagen dienen. Dies zeigt sich auch in anderen Beispielen aus dem deutschsprachigen Ausland, bei denen erfolgreiche Strafverfahren gegen Menschenhändler*innen geführt werden konnten, weil die Strafverfolgungsbehörden mithilfe von Audioaufnahmen und Social-Media-Nachrichten und Postings die Arbeitszeiten und -bedingungen, Transport und Logistik, das Tageseinkommen und die ständige Kontrolle, Bedrohung und Misshandlung der Betroffenen nachvollziehen konnten. Hier stützten digitale Beweise die Aussagen der Betroffenen, konnten diese aber nicht ersetzen.[128] Anzumerken ist, dass dies auch von Strafverfolgungsbehörden als Hindernis wahrgenommen wird und das Bundeskriminalamt mit seinen Verbundpartnern im Rahmen des Projektes »THB Liberi« seit 2018 auch an personenunabhängigen Beweisen in Menschenhandelsverfahren mit digitalen Komponenten arbeitet.

128 Siehe Chen, I./Tortosa, C.: The Use of Digital Evidence in Human Trafficking Investigations. In: Anti-Trafficking Review, Ausgabe 14, 2020, S. 122–124. https://doi.org/10.14197/atr.201220149.

Vorgehen gegen bildbasierte Gewalt ist nicht nur eine technologische Frage

Ein belastender Faktor für Frauen und Minderjährige, die auf einschlägigen Online-Portalen für die sexuelle Ausbeutung angeboten wurden, ist die Tatsache, dass selbst nach Beendigung der Ausbeutungssituation intime Aufnahmen von ihnen im Internet kursieren können. Das trifft auch auf Betroffene zu, von denen Täter*innen als Druckmittel online Nacktaufnahmen verbreitet haben. Bisher gibt es keine befriedigende Lösung, um solche Aufnahmen aufzufinden oder um sicherzustellen, dass solche Darstellungen nicht länger online zu finden sind. Zwar gibt es hashwertbasierte Lösungen, damit kann man jedoch nur bereits bekannte Bilder auffinden.[129] Daneben gibt es allgemein zugängliche Software zur Gesichtserkennung wie zum Beispiel PimEyes[130], die jedoch viele neue ethische Fragen bezüglich Datenschutz, Meinungsfreiheit und digitaler Überwachung aufwerfen.[131] »Alle Tools haben ihre Probleme, wenn sie rein maschinell laufen, ohne menschliche Kontrollinstanz. […] Es braucht auf jeden Fall eine Lösung für die Betroffenen bildbasierter Gewalt, die zuverlässig und datenschutzfreundlich funktioniert« (Interview bff). Bisher bleibt Beratungsstellen nichts anderes übrig, als mit den Betroffenen Wege zur Akzeptanz zu erarbeiten: »Ich muss damit leben, dass die Bilder da draußen sind.« Doch technologische Ansätze allein sind nicht die Lösung des Problems und dürfen nicht davon ablenken, dass diese Gewaltform in einem breiteren Kontext angegangen werden muss. »Wenn ich priorisieren müsste, ist eine ausreichende Finanzierung der Beratungsstellen und gut fortgebildete Staatsanwaltschaften und Polizei tausendmal wichtiger als zum Beispiel eine gute Bilderrückwärtssuchmaschine« (Interview bff). Das letztendliche Ziel sollte die Verhinderung solcher Gewalterfahrungen sein. Um dies zu erreichen, braucht es mehr als effektive Software, die intime Aufnahmen online auffindet. Vielmehr muss ein gesellschaftliches Klima geschaffen werden, in dem Täter*innen wissen, dass Strafverfolgung tatsächlich stattfindet.[132] Die Staatsanwaltschaft Berlin sieht Handlungsmöglichkeiten, wenn Nacktaufnahmen im Kontext eines Menschenhandelsfalls von Täter*innen gegen den Willen der Geschädigten veröffentlicht werden, da dies ggf. als Erpressung, Bedrohung oder versuchte Nötigung zumindest mit Geldstrafen geahndet werden kann. »Zwar tritt der Strafrahmen der Erpressung, Bedrohung oder Nötigung hinter dem des schweren Menschenhandels oder der schweren Zwangsprostitution zurück, jedoch finden diese mitverwirklichten Delikte Berücksichtigung im Rahmen der Strafzumessung« (Interview Staatsanwaltschaft Berlin). Die Krux sei allerdings auch hier, dass die Nachweisbarkeit vorhanden sein muss, um anklagen und verfolgen zu können.

129 Ein Hashwert ist ein digitaler Code aus Zahlen und Buchstaben und kann vereinfacht gesagt als digitaler Fingerabdruck eines Bildes verstanden werden. Listen mit bekannten Hashwerten werden für das Aufspüren von Missbrauchsabbildungen von Kindern in Webdiensten von Microsoft, Google, Facebook, Twitter, Adobe Inc. und anderen Firmen eingesetzt, die Verdachtsfälle den entsprechenden Behörden melden. Das bekannteste und auch in Deutschland eingesetzte Tool ist PhotoDNA von Microsoft. »Dazu wird das Bild in ein Schwarz-Weiß-Bild gewandelt, verkleinert und mit einem Raster in Einzelbilder zerlegt. Jedes Einzelbild wird nach dem stärksten Gradienten abgesucht. Die Gradienten aller Bilder zusammen ergeben die PhotoDNA.« (https://www.wikiwand.com/de/PhotoDNA).

130 PimEyes: https://pimeyes.com/en.

131 Für eine kritische Auseinandersetzung mit Tech-Tools in der Menschenhandelsbekämpfung siehe auch Anti-Trafficking-Review Ausgabe 14, 2020 »Special Issue – Technology, Anti-Trafficking, and Speculative Futures«. https://www.antitraffickingreview.org/index.php/atrjournal/issue/view/22. Darin geben Milivojevic, S./Moore, H./Segrave, M. bzgl. Gesichtserkennungstools zu bedenken: »Neben der neuesten Version von Razzia und Rettung [raid and rescue] haben wir auch den Anstieg der Gesichtserkennung als eine Technologie gesehen, die bei der Identifizierung von Opfern von Menschenhandel und Sklaverei helfen kann. Bedenken über die Grenzen und Folgen solcher Technologien werden durch den überwältigenden moralischen Imperativ ›Schützen und Retten‹ zum Schweigen gebracht. Die Macht dieses moralisierenden Diskurses ist so groß, dass er durch das Fehlen von Beweisen, die diese Position stützen, unberührt bleibt.«

132 Siehe auch die Broken-Web-Theorie von Dr. Thomas-Gabriel Rüdiger u. a. »Das Broken-Web-Phänomen«. In: Jur@ im Netz, Dezember 2017.

IT-Kompetenzlücken und Social-Media-Berührungsängste bei Fachberatungsstellen

In Fachberatungsstellen arbeiten in der Regel Fachkräfte aus Sozialer Arbeit, Sozialwissenschaften und Psychologie mit geringen IT-Kenntnissen, und die meisten Beratungsstellen des KOK sind kleine Organisationen ohne eigene IT-Abteilung, die nur bei Bedarf von externen IT-Spezialist*innen unterstützt werden. Wissen fehlt in der gesamten Spannbreite technischer und technologischer Aspekte, von einer Grundsensibilisierung über IT-Sicherheit von Klient*innen und Beraterinnen bis hin zu digitaler Beweissicherung. »Täter nutzen Lücken aus, und wenn wir digital unterwegs sind, muss man das auch mitdenken. Wo muss man aufpassen und sich technisch schützen, und wie?« (Interview FBS). Angriffe auf Computersysteme von Fachberatungsstellen kommen immer wieder vor. Bisherige Schulungen decken vornehmlich den Bereich Datenschutz ab, doch tiefergehende Fortbildungen zu IT-Sicherheit sind notwendig und erwünscht: »Wir brauchen eigentlich alles« (Interview FBS). Der bff als eine Nichtregierungsorganisation, die gegen geschlechtsspezifische Gewalt an Frauen arbeitet, bietet als einer der wenigen Akteure in diesem Feld spezielle Schulungen im Rahmen des Projektes »aktiv gegen digitale Gewalt« an, die so gut im Verbund angenommen werden, dass die Mitarbeiterinnen »der Nachfrage kaum hinterherkommen« (Interview bff).

Diese IT-Lücke scheint auch generationsbedingt zu sein. Ältere Beraterinnen zeigen in der Regel weniger Technikaffinität und mehr Berührungsängste mit digitalen Medien als jüngere Kolleginnen und Praktikantinnen. Manche Fachberatungsstellen bedienen aus Datenschutzgründen überhaupt keine Social-Media-Kanäle, andere treten diese unliebsame Aufgabe an jüngere Beraterinnen ab, da sie als sog. *digital natives*, die mit dem Internet und sozialen Medien groß geworden sind, häufig als automatisch befähigter angesehen werden. Obwohl es in der praktischen Umsetzung herausfordernd ist, sind sich die meisten Fachberatungsstellen dieser Hürde und der Handlungsnotwendigkeit bewusst: »Als Beratungsstelle muss man sich schulen, sich fortbilden, um sich up to date zu bringen. Aber man muss auch die personellen Ressourcen und die Zeit haben, sich mit der ganzen Sache auseinanderzusetzen. Will ich einen Facebook-Account haben? Was möchte ich damit, was ist mein Ziel, wie möchte ich es nutzen? Wenn man es selbst [privat] nicht nutzt und darin versiert ist, ist es eine Hürde im Kopf, damit anzufangen« (Interview FBS). In der Praxis scheint bisher eine Lösung zu sein, unterschiedliche Altersstufen der Beraterinnen in die personelle Struktur einzubauen.

Mangelndes Bewusstsein für technologieabgeleitete Risiken bei Betroffenen

»Ich bin immer wieder erstaunt, wie gut die Klientinnen mit Apps umgehen und technisch fit sind, aber gleichzeitig in deren Einsatz so unbekümmert sind. Sensibilität und Achtsamkeit fehlt« (Interview FBS). Ein wenig auf Schutz der Privatsphäre gerichteter Umgang mit sozialen Medien wird von vielen Fachberatungsstellen beobachtet, selbst bei Klientinnen, die in Schutzunterkünften untergebracht sind und akute Bedrohung durch die Menschenhändler*innen befürchten. Betroffene posten Bilder, die Hinweise auf ihre Umgebung und ihren Aufenthaltsort geben, z. B. von charakteristischen Plätzen einer Stadt. Die Sensibilisierung von Klientinnen für die damit verbundenen Gefahren und für einen besseren Schutz der eigenen Privatsphäre als auch der Sicherheit der gesamten Schutzunterkunft scheint bisher mühsam. Beraterinnen führen dies auf die grundlegende Charakteristik der Klientin-Beraterin-Beziehung zurück, in der ein Vertrauensaufbau viel Zeit erfordert. Erst wenn Betroffene sehen, dass die Versprechen und Absprachen mit den Beraterinnen in der Praxis tatsächlich helfen, legen sie ihre Skepsis ab. Für Unterstützung im digitalen Raum gilt nun das Gleiche: »Die Kunst ist es, dies auf die digitale Welt zu transferieren« (Interview FBS).

Ein unbewusst risikoreicher Umgang der Betroffenen mit Social Media zeigt sich auch in andere Richtungen. Eine Fachberatungsstelle hat mit der Situation zu tun, dass eine Klientin in der Absicht abzuschrecken ein Video mit Missbrauchsabbildungen von Kindern, das sie erhalten hatte, auf ihrem Social-Media-Account gepostet hat – und nun Ermittlungen wegen Verbreitung von kinderpornografischem Material gegen sie laufen. Zudem sind Beraterinnen neuen Belastungen ausgesetzt, wenn sie sich zur Beweissicherung einer Bedrohung der Klientin durch die Täter*innen Gewaltvideos ansehen müssen, die Mord oder brutalste körperliche Gewalt zeigen.

Neue Dilemmata in der digitalen Sozialen Arbeit

Immer mehr FBS machen sich auf den Weg hin zu Online-Beratungsangeboten oder digitaler Streetwork.[133] Neben neuen Fertigkeiten bezüglich dafür angewandter Technologie und deren Wartung bringt die Digitalisierung Sozialer Arbeit jedoch auch neue Dilemmata mit sich. Eines davon wird anhand eines konkreten Fallbeispiels deutlich: Eine FBS wird von zwei Mädchen, beide 13 Jahre alt, kontaktiert. Sie melden sich, getrennt voneinander, mit der Bitte um anonyme Online-Beratung. In einem Fall über TikTok, in dem anderen Fall über Twitch pirschten sich erwachsene Männer an die Kinder heran, umschwärmten sie und versuchten, die Mädchen mit der Loverboy-Strategie zu manipulieren, um Nacktbilder von ihnen zu bekommen. In einem der beiden Fälle handelte es sich beim Tatverdächtigen um einen Mann in Algerien. »Es war absehbar, wohin der Fall geht. Wenn wir das aber melden, dann sind die Mädchen weg. Dieses Dilemma hatten wir auch immer schon beim Streetwork. In der Arbeit mit Minderjährigen ist der Vertrauensaufbau sehr wichtig. Schalten wir das Jugendamt oder die Polizei direkt ein, um die Betroffenen von der Straße zu holen, wird das nicht funktionieren. Zudem ist die genaue Identität meistens erst mal nicht bekannt. Die Kinder und Jugendlichen werden in dem Fall verschwinden und den erneuten Kontakt zu den Streetworkerinnen vermeiden. Eine Intervention wird so verhindert. Greifen die Polizei oder das Jugendamt ein und bringen die Betroffenen nach Hause oder in eine Jugendschutzstelle, verbleiben sie in der Regel nur sehr kurz dort und sind dann wieder auf der Straße anzutreffen. Dieses Dilemma ist auch den Behörden bewusst. Und da sind wir in der Online-Beratung noch nicht so erfahren, wie wir richtig damit umgehen, denn nicht nur wir, sondern auch der Täter hält ja die ganze Zeit den Kontakt zu den Mädchen aufrecht« (Interview FBS).

Zudem birgt digitale Streetwork (mindestens) eine weitere Frage, nämlich wie mit geografischen Zuständigkeiten und der Erreichbarkeit umgegangen werden soll. Wenn in der analogen Streetwork eine Frau anruft, die sich aus einer Ausbeutungssituation befreien konnte, und unmittelbar um Abholung an einem vereinbarten Standort bittet, wird die Beraterin meist dorthin kommen. Dies findet bisher auf regionaler Ebene statt. Fachberatungsstellen haben noch keine erprobte Handhabe, wie das bei Online-Angeboten zu lösen ist, wenn sich beispielsweise Hilfesuchende aus anderen Bundesländern in akuten Situationen bei ihnen melden. Auch die Frage nach einer möglichen 24/7-Erreichbarkeit von Online-Unterstützungsangeboten ist noch unklar.

133 Ergebnisse eines KOK-Events für seine Mitgliedsorganisationen, 06.09.2022

Relevanz konkurrierender Themen

So wichtig die Beschäftigung mit dem Technologieeinsatz im Menschenhandel auch sei, äußerten mehrere Befragte die Sorge, sie würde als neues »Modethema« sämtliches politische Interesse auf nur diesen einen Ausschnitt eines in Wahrheit viel komplexeren Themenbereichs lenken: »Was ich ein bisschen befürchte, ist, wenn das Digitale mehr und mehr in den Fokus kommt, dass der analoge Teil darunter leidet« (Interview FBS). Eine Befragte zog beispielhaft die Analogie zur Thematik Missbrauchsdarstellungen von Kindern: Nach genügend pressewirksamen Fällen sei die Politik darauf angesprungen, finanziere Projekte und verabschiede Maßnahmen, doch es gebe kein politisches Interesse, Kinderschutz als Ganzes zu fördern. Ähnliches war im Frühling 2022 am Beispiel Menschenhandel aus der Ukraine zu beobachten. Die politische und gesellschaftliche Aufmerksamkeit war auf die Risikogruppe der Ukrainerinnen gerichtet, während sich nichts an der prekären Situation anderer vulnerabler Personen als (potenziell) Betroffene des Menschenhandels geändert hat. »Man muss seit dem Ukrainekrieg immer daran erinnern, dass es die anderen Themen auch noch gibt« (Interview FBS).

Langsame Digitalisierung der Justiz

Ein großes Hindernis in der aktuellen Bekämpfung des Menschenhandels in Deutschland ist die nur langsam erfolgende Digitalisierung der Justizbehörden. Bei grenzüberschreitenden Fällen schickt die Staatsanwaltschaft Rechtshilfeersuchen in Form einer schriftlichen Anordnung ins Ausland. Die Antwort dauert im Schnitt drei Monate, bis es dann zu einer Anklage kommt, können mehrere Monate vergehen. Falls Nachermittlungen notwendig sind, erhöht sich dieser Zeitraum sogar noch. Die Nachteile für die Betroffenen liegen auf der Hand: »Wenn eine Frau bedroht wird, sind drei Monate eine Ewigkeit. Das ist eine Zumutung für die Geschädigten.« Für die Justizbehörden kann eine lange Prozessdauer in Folge bedeuten, dass sie ihre Opferzeugin möglicherweise verlieren, »[...] dann ist die Frau nicht mehr greifbar. Wenn es möglich wäre, Erkenntnisse aus dem Ausland auf kurzem Wege verwertbar zu machen, z. B. in Form eines E-Mail-Ausdrucks, der zur Akte genommen wird, könnte eine Beschleunigung erreicht werden« (Interview Staatsanwaltschaft Berlin). Eine elektronische Akte würde dies begünstigen, so die Berliner Staatsanwaltschaft, doch es scheint noch ein langer Weg bis dahin, da viele Vorbehalte innerhalb des Justizsystems bestehen: »Digitalisierung kann neue Angriffspunkte bieten, was Datenmissbrauch anbelangt. Dies ist bei einer ›körperlichen‹ Akte, welche von Hand zu Hand gereicht werden muss, nicht der Fall. Die Sorge verstehe ich, aber technologiegestützte Ermittlungen sind wirklich ein Zeitfaktor. Und gerade bei Menschenhandelsfällen spielt Zeit eine Rolle.« Die IT-Sicherheitsstrukturen in Staatsanwaltschaften erschweren es zudem, nicht den Anschluss an technologische Entwicklungen zu verpassen. Bei der Berliner Staatsanwaltschaft beispielsweise können USB-Sticks und Daten-CDs nicht ohne Weiteres am eigenen Rechner gelesen werden. Es ist davon auszugehen, dass die Situation im Rest des Landes ähnlich ist. Wenn Staatsanwält*innen sich nun mit einer neuen App oder einer neuen Software vertraut machen wollen, die für das jeweilige Verfahren relevant ist, können sie das erst mithilfe der eigenen IT-Abteilung tun. »Die Staatsanwaltschaft hinkt diesbezüglich den Tätern häufig hinterher« (Interview Staatsanwaltschaft Berlin).

7

AUSGEWÄHLTE BEISPIELE TECHNOLOGIEBASIERTER LÖSUNGSANSÄTZE

Fachberatungsstellen des KOK haben die Covid-19-Pandemie zum Anlass genommen, neben dem regulären Webauftritt ihre Hilfsangebote weiter zu digitalisieren. Sie haben ihre Onlinepräsenz in sozialen Netzwerken verstärkt und bieten zunehmend auch Online-Beratung an, die eine größere Reichweite, bessere Erreichbarkeit für die Klient*innen durch lokale Unabhängigkeit und mehr Niedrigschwelligkeit und schnellere Reaktionsfähigkeit der Beraterinnen ermöglicht. Zudem adaptieren erste Fachberatungsstellen das Konzept der digitalen aufsuchenden Arbeit, auch *digital Streetwork* genannt.[134] Darüber hinaus konnten bisher keine technisch versierten oder technologisch innovativen Ansätze identifiziert werden.

Im Folgenden werden vier Lösungsansätze vorgestellt, die auf unterschiedlichen technologischen Konzepten basieren (Website, Machine Learning, Virtual Reality und App). Doch die internationale Entwicklung von technologiebasierten Tools schreitet immer schneller voran. Während 2009 noch durchschnittlich fünf Tools jährlich veröffentlicht wurden, sind es seit 2015 im Schnitt 40.[135] Die folgenden Beispiele sollen daher nur als Veranschaulichung des Spektrums der existierenden Möglichkeiten dienen. Auf eine umfassendere Betrachtung hingegen wird verzichtet, da anzunehmen und sogar zu hoffen ist, dass wir in naher Zukunft noch mit mehr, effektiveren und technisch weiter ausgereiften Instrumenten gegen Menschenhandel rechnen können.

bff-Handlungsanleitungen gegen digitale Gewalt an Frauen

Der bff – Frauen gegen Gewalt e. V. hat eine themenspezifische Website »Aktiv gegen digitale Gewalt«[136] eingerichtet, auf der die bisher relevantesten und bekannten Gewaltformen, u. a. Cyberstalking, bildbasierte sexualisierte Gewalt und Identitätsdiebstahl, aufgegriffen werden. Jede Ausprägung wird begleitet von definierenden Erklärungen, Informationen über die relevanten Straftatbestände, die für die jeweilige Gewaltform Anwendung finden können, und Handlungsempfehlungen für Betroffene. Daneben beinhaltet die Webseite eine eigene Kategorie zu Techniksicherheit und Privatsphäre, in der u. a. eine konkrete Anleitung zur Sicherung digitaler Beweismittel gegeben wird.

134 Informationen aus einer KOK-Online-Fortbildung für Mitgliedsorganisationen am 06.09.2022; als Beispiel einer Umsetzung von digital Streetwork im Jungendhilfebereich siehe https://www.digital-streetwork-bayern.de.

135 OSCE, 2020: Leveraging innovation to fight trafficking in human beings: a comprehensive analysis of technology tools, S. 23.

136 bff: https://www.aktiv-gegen-digitale-gewalt.de/de/digitale-gewalt/bildbasierte-sexualisierte-gewalt/was-kann-ich-tun.html.

Per Webcrawler gegen Prostitutionsanzeigen mit Minderjährigen: ein Tool des BKA-Projektes »THB Liberi«

Bei Sexanzeigen geben bestimmte Schlagworte Hinweise, dass es sich bei den annoncierten Personen um Minderjährige handeln könnte, was ein Ausgangspunkt für polizeiliche Ermittlungen sein kann. Um nicht händisch nach diesen spezifischen Formulierungen und Informationen suchen zu müssen, setzen das BKA und inzwischen 60 Polizeidienststellen in Deutschland einen sogenannten Webcrawler ein. Ein Webcrawler ist vereinfacht gesagt ein Computerprogramm, das öffentlich zugängliche Webseiten automatisch nach bestimmten Inhalten durchsucht. Dieser aktuell in Deutschland von der Polizei eingesetzte Webcrawler ist ein Bestandteil neuer Lösungsansätze, die das BKA im Rahmen des aus dem Inneren Sicherheitsfonds geförderten Projektes »THB Liberi« mit acht Partnerdienststellen in Deutschland und dem österreichischen Bundeskriminalamt seit dem Jahr 2018 entwickelt. »THB Liberi« dient der Bekämpfung des Menschenhandels und der Ausbeutung Minderjähriger in Deutschland und Europa mittels eines verbesserten multidisziplinären Ansatzes zwischen Staaten, Behörden und Nichtregierungsorganisationen. Menschenhandel mithilfe des Internets, darin spezifisch die Online-Anwerbung Jugendlicher und Heranwachsender, ist ein dezidierter Fokus des Projektes.[137] Die Laufzeit wird mithilfe der Förderung über das Nationale Programm um 2023–2025 verlängert, wobei der Fokus auch weiterhin auf internetgestütztem Menschenhandel liegen soll.[138]

Virtuelle Realität als Übungsfeld für angehende Fachkräfte

Die Psychologische Hochschule Berlin entwickelt zusammen mit den Verbundpartnern Europa-Universität Flensburg und der Universitätsmedizin der Georg-August-Universität Göttingen seit 2018, aktuell in der zweiten Projektphase bis 2024, ein sog. Training in virtueller Umgebung zur Befragung bei Verdacht auf sexuellen Missbrauch – das Projekt ViContact 2.0. Die Zielsetzung des Projektes ist zum einen die Vorbereitung von Lehramtsstudierenden, Lehrkräften und Personen aus dem Kinderschutzbereich auf Erstgespräche in Verdachtsfällen sexualisierter Gewalt an Kindern. Zum anderen geht es um die Entwicklung eines handlungsorientierten Gesprächstrainings für das Erlernen von suggestionsfreien, unterstützenden Gesprächen mit Kindern.[139] Lernende führen Gespräche mit virtuellen Avataren, die vom Aussehen und Gesprächsverhalten her etwa zehnjährigen Kindern entsprechen. Diese verfügen über programmierte Gedächtnisinhalte in Form narrativer Antworten, die sie bei angemessener (d. h. einerseits unterstützender, andererseits aber auch ergebnisoffener, nicht-suggestiver) Befragung preisgeben. Noch müssen menschliche Operator*innen im Hintergrund Elemente des Gesprächs manuell kodieren, an einer KI-Version wird gearbeitet. Im Anschluss an die Gespräche erhalten die Lernenden ein automatisiertes, personalisiertes Feedback. Das Projekt wird in der laufenden Phase evaluiert.

Die Hochschule der Polizei Rheinland-Pfalz[140] nutzt VR-Brillen in der Ausbildung von Polizeibeamt*innen, um mögliche Betroffene des Menschenhandels in Prostitutionsausübungsstätten zu erkennen. In Kontrollszenarien können die Lernenden üben, auf welche Hinweise z. B.

137 Kramer, F. 2020: Mit THB Liberi organisierten Menschenhandel bekämpfen. In: Die Polizei, 11-2020.

138 Schriftliche Informationen vom BKA, Juli 2022.

139 Tamm, A./Volbert, R., Präsentation vom 10.05.2022: Das Projekt ViContact. Befragungen bei Verdacht auf sexuellen Missbrauch – Training in virtueller Umgebung.

140 Forschung an der Hochschule der Polizei Rheinland-Pfalz. https://www.polizei.rlp.de/de/die-polizei/ueber-uns/dienststellen/hochschule-der-polizei-rheinland-pfalz/forschung/.

bei Bordellkontrollen zu achten ist. Allerdings sind die VR-Szenarien nicht KI-unterstützt, d. h. es ist keine Interaktion mit den Frauen möglich, da sie nicht reagieren können.

Wirtschaftlichkeit als Entscheidungsgrundlage: Pacific-Links-App PAXU zur Prävention von Arbeitsausbeutung

Die US-basierte und in Vietnam gegen Menschenhandel tätige Nichtregierungsorganisation Pacific Links Foundation hat eine App entwickelt, die vermeintliche Arbeitsangebote und versprochene Löhne im Ausland mit den tatsächlichen Lebenshaltungskosten des jeweiligen Landes, kalkulierter Schuldentilgung und den benötigten Dokumenten für eine sichere Migration vergleicht.[141] Statt Prävention mithilfe von Warnungen über Risiken und Gefahren von Menschenhandel zu betreiben, setzt dieser Ansatz auf eine einfache Kosten-Nutzen-Rechnung, denn Arbeitsmigration ist eine wirtschaftliche Entscheidung. Bisher ist die App nur auf Englisch und Vietnamesisch verfügbar und wird in den Online-Communitys auf entsprechenden Facebook- und in Messenger-Gruppen bekannt gemacht.

Neben diesen beispielhaft vorgestellten Lösungen, die auf Technologien basieren, gibt es eine ganze Reihe weiterer digitaler oder technologiegestützter Tools in der Anti-Menschenhandels-Sphäre weltweit. Die Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) hat zusammen mit der Organisation »Tech against Trafficking« 300 von diesen Tools in einem im Juni 2020 veröffentlichten Bericht analysiert.[142]

Technologiebasierte Lösungen vs. der Kern des Problems

Technologien sind ein Teil des Problems und müssen daher auch ein Teil der Lösung sein. Doch sie dürfen nicht vom grundlegenden Diskurs um die Bedingungen in Gesellschaften ablenken, die Menschenhandel überhaupt erst ermöglichen oder gar verschärfen, wie zum Beispiel Migrationspolitiken, Ungleichheitsverhältnisse, Genderbenachteiligung – all dies sind Faktoren, die unabhängig von Technologien betrachtet werden müssen.[143] Es steht außer Frage, dass Maßnahmen zur Menschenhandelsbekämpfung die Möglichkeiten von IKTs weiter erforschen und ausprobieren sollten, für Prävention und Strafverfolgung und v. a. um Betroffene schneller aus Ausbeutungssituationen zu helfen und sie besser zu schützen und unterstützen. Doch weder sollten dabei das Internet und IKTs zum Sündenbock für diese Verbrechen gemacht werden, noch sollte auf sie als Heilsbringer aller Maßnahmen gebaut werden. Mehr kritische Forschung zum Impact technologiebasierter und -gestützter Ansätze ist notwendig.

Eine technologiebasierte Bekämpfung des Menschenhandels und Unterstützung der Betroffenen birgt zudem auch menschenrechtliche Risiken wie Überwachung der Betroffenen, Einschränkung ihrer Bewegungsfreiheit und Reduzierung ihrer Handlungsfähigkeit, die unter die Notwendigkeit, »gerettet« zu werden, gestellt werden.[144] Zudem wirft der Einsatz von Informations- und Kommunikationstechnologien in der Menschenhandelsbekämpfung, der auf der Grundlage von Daten operiert, erhebliche datenschutzrechtliche Fragen auf. Der KOK beschäftigt sich seit 2012 mit dem

141 Pacific Links Foundation: PAXU. https://pacificlinks.org/paxu/#Courage.

142 OSCE, 2020: Leveraging innovation to fight trafficking in human beings: a comprehensive analysis of technology tools.

143 Vgl. Milivojevic, S./Moore, H./Segrave, M.: Freeing the Modern Slaves, One Click at a Time: Theorising human trafficking, modern slavery, and technology. In: Anti-Trafficking Review, Ausgabe 14, 2020, S. 16–32.

144 Vgl. ebd.

komplexen Themenbereich von Datenschutz und Datensammlung und deren Auswirkungen auf Betroffene des Menschenhandels und hat dazu mehrere Publikationen veröffentlicht.[145]

8

EMPFEHLUNGEN UND AUSBLICK

In dieser Studie wurden Notwendigkeiten, Lücken und Hindernisse herausgearbeitet, die für die unterschiedlichen Akteur*innen relevant sind, die in Deutschland für die Verhinderung und Bekämpfung des Menschenhandels und für die Unterstützung der Betroffenen zuständig sind. Daraus lassen sich einige grundsätzliche Empfehlungen für Politik, Strafverfolgung und Fachberatungsstellen ableiten.

Politik: Cybersicherheitsagenda um Menschenhandel erweitern und einheitliche Definition einführen

Das Bundesministerium des Innern und für Heimat (BMI) hat im Juni 2022 eine Cybersicherheitsagenda[146] mit Zielen und Maßnahmen für die 20. Legislaturperiode veröffentlicht, die den »ressortübergreifenden strategischen Rahmen für die Aktivitäten der Bundesregierung mit Bezügen zur Cybersicherheit«[147] darstellt. Darin finden sich zwar im Kapitel »Cybercrime und strafbare Inhalte im Internet bekämpfen« eine Reihe von Maßnahmen gegen sexualisierte Gewalt an Kindern inkl. Missbrauchsdarstellungen im Internet, doch der technikgestützte Menschenhandel findet weder in diesem Kapitel noch an anderer Stelle Erwähnung. Für eine umfassende Verhinderung und Bekämpfung des zunehmend digitalisierten Menschenhandels wird empfohlen, das Thema in die nächste Cybersicherheitsagenda der Bundesregierung aufzunehmen.

Zudem unterscheidet sich die BMI-Definition[148] von Cybercrime von der des Bundeskriminalamts, und die wiederum von der Definition, die das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt.[149] Wie in Kapitel 2 gezeigt können unterschiedliche Definitionen dieser Straftaten ein Hinderungsgrund für effektive Maßnahmen sein. Ein einheitliches Verständnis sollte geschaffen werden und als Grundlage aller Maßnahmen dienen. In die Entwicklung einheitlich akzeptierter Definitionen, v. a. im Hinblick auf digitalisierte Elemente des Menschenhandels, sollten auch weitere Akteur*innen aus Wissenschaft, strafrechtlicher und justizieller Praxis und Nichtregierungsorganisationen einbezogen werden.[150]

145 Bundesweiter Koordinierungskreis gegen Menschenhandel – KOK e. V., 2020: Defining the Gap: Datenerhebung zu Menschenhandel und Ausbeutung in Deutschland – der zivilgesellschaftliche Ansatz des KOK; Projektwebseite datACT: https://www.kok-gegen-menschenhandel.de/datenschutz-datact; Uhl, B.: Daten und Verantwortung – Betrachtungen zur Datafizierung, Zivilgesellschaft und Anti-Menschenhandelsarbeit. In: KOK e. V., 2020: Menschenhandel in Deutschland – Rechte und Schutz für Betroffene, S. 250–257.

146 BMI, Juni 2022: Cybersicherheitsagenda.

147 BMI: IT- und Cybersicherheit. https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/it-und-cybersicherheit-node.html.

148 BMI: Definition von Cyberkriminalität: Cyberkriminalität ist ein weltweites Phänomen, das weder an Landesgrenzen noch vor verschlossenen Türen Halt macht. Sie kann überall stattfinden, wo Menschen Computer, Smartphones und andere IT-Geräte benutzen – in Firmen, Behörden, Universitäten, zu Hause und unterwegs. Straftaten, bei denen die Täter moderne Informationstechnik nutzen, werden zunächst ganz allgemein als Cyberkriminalität (engl. cybercrime) bezeichnet. Cyberkriminalität ist zum Beispiel ein Betrugsversuch, der das potentielle Opfer via E-Mail statt per Post erreicht. Im engeren Sinne umfasst der Begriff jedoch Straftaten, die auf Computersysteme und Netzwerke selbst zielen. Dabei kann es sich auch um Cyberspionage oder Cyberterrorismus handeln. https://www.bmi.bund.de/DE/themen/sicherheit/kriminalitaetsbekaempfung-und-gefahrenabwehr/cyberkriminalitaet/cyberkriminalitaet-node.html.

Politik: Digitalisierung der Behörden zügig vorantreiben

Um bei der stetigen Weiterentwicklung krimineller Machenschaften im Bereich technologiegestützter Menschenhandel wettbewerbsfähig zu werden, muss die Bundesregierung die Digitalisierung aller Behörden schneller als bisher vorantreiben und dahingehende Vorhaben wie die Digitalstrategie[151] vollumfänglich umsetzen.

Politik: Zuständigkeiten für das Thema technologiegestützter Menschenhandel klären und multidisziplinäre Zusammenarbeit erleichtern

Obwohl die vorliegende Studie die Perspektive und Erfahrungen der Fachberatungsstellen zum Mittelpunkt hat, war auch beabsichtigt, die politische Ebene zum Thema zu befragen. Menschenhandel und insbesondere die digitale Dimension des Phänomens sind Querschnittsthemen, die verschiedene Ressorts betreffen. Die Zuständigkeiten hier müssen noch etwas geschärft werden. Im Bundesinnenministerium kommen zwei Referate als Ansprechpartner infrage, zum einen das Referat CI 8 zu Cyberfähigkeiten des Bundeskriminalamtes, dessen Fokus allerdings eher auf Missbrauchsabbildungen und sexualisierter Gewalt gegen Kinder online liegt.

Zum anderen das Referat ÖS II zu schwerer und organisierter Kriminalität, welches zwar für das Thema Menschenhandel zuständig ist, das jedoch (noch) über keine Expertise zu technologiegestützten Aspekten der Thematik verfügt. Diskussionen zu möglichen Schnittflächen beider Themenfelder haben im Herbst 2022 mit beiden Referaten im Rahmen der deutschen G7-Präsidentschaft stattgefunden. Dies ist ein vielversprechender Ansatz und sollte unbedingt weitergeführt werden. Insgesamt sollten die Zuständigkeiten klarer benannt und verteilt und, wo notwendig, Strukturen für eine multidisziplinäre Zusammenarbeit geschaffen werden. Ansonsten besteht die Gefahr, dass es alle theoretisch als Querschnittsthema sehen, praktisch aber niemand dafür verantwortlich ist.

Politik: Technologieunternehmen rechtlich in die Verantwortung nehmen

Webseiten und Plattformen, die auch von Menschenhändler*innen zur Bewerbung von Betroffenen genutzt werden, werden in Deutschland bisher kaum für die Inhalte zur Rechenschaft gezogen. Die Bundesregierung sollte diese Rechtslücke schließen, indem sie Rechenschafts- und

149 BSI: Methoden der Cyber-Kriminalität: Cyber-Kriminalität (engl. cybercrime) bezeichnet alle Straftaten, die moderne Informationstechnik und elektronische Infrastrukturen (aus-)nutzen. Die Bandbreite von Straftaten im Bereich Cyber-Kriminalität wächst stetig an. Durch die fortschreitende Digitalisierung der Gesellschaft entstehen immer neue IT-Anwendungen in unserem Alltag. Damit gehen potenzielle Sicherheitslücken unweigerlich einher. Zu den am weitesten verbreiteten Methoden von Cyber-Kriminalität gehören u. a. : Schadprogramme (und alle Unterarten) sowie Emotet, Identitätsdiebstahl durch Doxing, Spam und Phishing, Botnetze, Social Engineering. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/methoden-der-cyber-kriminalitaet_node.html.

150 Vergleichbare Abstimmungsprozesse sind im Rahmen der Erstellung des Terminologischen Leitfadens für den Schutz von Kindern vor sexueller Ausbeutung und sexualisierter Gewalt im Jahr 2017 unter der Leitung von ECPAT Deutschland e. V. erfolgt.

151 Digitalstrategie der Bundesregierung: https://digitalstrategie-deutschland.de/ueber-die-digitalstrategie/.

Haftungsmechanismen für Technologieunternehmen für Schäden einführt, die durch Inhalte auf ihren Plattformen oder die Nutzung ihrer Plattformen verursacht werden.[152]

Politik: IT-Infrastruktur bei Finanzierung von Fachberatungsstellen berücksichtigen

Betroffene von Menschenhandel und Ausbeutung haben einen Schutzanspruch gegenüber dem Staat. Kann der Staat eine Rechtsverletzung nicht verhindern, ergibt sich daraus das Recht auf Beratung und Unterstützung. Dem kann nur entsprochen werden, wenn eine stabil finanzierte Unterstützungsstruktur existiert. Der KOK fordert seit Jahren eine sichere und langfristige finanzielle Förderung spezialisierter Fachberatungsstellen.[153] Anders als bisher muss die finanzielle Ausstattung auch den Aufbau, die Pflege und die Weiterentwicklung sicherer IT-Infrastrukturen und entsprechende Schulungen der Beraterinnen beinhalten. Das ermöglicht die Erweiterung des Wirkkreises von Fachberatungsstellen in digitale Umgebungen, in denen sich auch Täter*innen zur Anwerbung potenzieller Betroffener bewegen. Gleichzeitig schützen stabile und sichere IT-Systeme und geschulte Beraterinnen sowohl die Organisationen als auch einzelne Mitarbeiterinnen vor Cyberangriffen.

Strafverfolgungsbehörden: Sensibilität, IT-Kompetenzen und Ressourcen ausbauen

Die Cybersicherheitsagenda des BMI sieht einen Ausbau von IT-Kompetenzen unterschiedlicher Behörden zur Bekämpfung von Cybercrime vor und fokussiert dabei insbesondere die Abteilung Cybercrime beim BKA und den Ausbau der Ermittlungsfähigkeiten der Bundespolizei in diesem Phänomenbereich durch personelle und technische Stärkung.[154] Der Bereich technologiegestützter Menschenhandel sollte dringend in diesen Kompetenzausbau einbezogen werden. Um dem Rechtsanspruch von Betroffenen auf Schutz und Hilfe nachkommen zu können, müssen die Strafverfolgungsbehörden in Deutschland u. a. eine neue Sensibilität und Offenheit dem Thema gegenüber entwickeln, digitale Gewaltformen verstehen und operative Fähigkeiten für Ermittlungen und zur digitalen Spurensicherung erwerben. Dafür brauchen sie mehr Ressourcen, und zwar nicht nur in den Cybercrimeabteilungen, sondern auch in den Abteilungen zu Menschenhandel, wo die technologiegestützten Elemente nur einen Teil der Straftat ausmachen. Zudem bedarf es diesbezüglich stärkerer und zum Teil neuer innerbehördlicher und multidisziplinärer Kooperationen.

Fachberatungsstellen: IT-Sicherheit erhöhen und IKT-Schutzkonzepte erweitern

Angesichts einer immer stärkeren Präsenz und Aktivität in digitalen Umgebungen müssen sich Fachberatungsstellen hinsichtlich einer sicheren IT-Infrastruktur besser aufstellen. Hier gilt es insbesondere, eigene IT-Kompetenzen aufzubauen und eine stabile Finanzierung dafür zu sichern. Ein Beispiel für einen vielversprechenden Ansatz, dessen Umsetzung weiterverfolgt werden sollte, ist die Zusammenarbeit einiger bff-Beratungsstellen mit IT-Fachkräften im Projekt InterAktion.[155]

Darüber hinaus sollten die Fachberatungsstellen ihr Schutzkonzept für Klient*innen, v. a. in Schutzunterkünften, um spezifische Elemente erweitern, die sich aus dem Gebrauch von Informations- und Kommunikationstechnologien ergeben. Die Frage nach der Smartphone-Nutzung der Betroffenen in sicheren Unterkünften ist nicht neu, gewinnt aber zunehmend an Komplexität durch die sich entwickelnde Technik. Es geht nicht mehr nur darum, dass Klientinnen zu Menschenhändler*innen nicht aktiv per Telefon, SMS oder WhatsApp Kontakt aufnehmen sollen oder wie sie verhindern können, von diesen ungewollt kontaktiert zu werden. Inzwischen geht es auch um die Frage nach versteckter Spyware, GPS-Standortermittlung und weiteren Apps, durch die Menschenhändler*innen weiterhin Zugriff auf und Kontrolle über die Betroffenen haben können. Dies schließt auch einen reflektierten Umgang der Betroffenen mit Social-Media-Kanälen und Profilen mit ein. Aus Sicht der Fachberatungsstellen ergibt sich daraus ein Dilemma, in dem zwischen Sicherheit und der Privatsphäre und *agency* der Klientinnen abgewogen werden muss. Hier könnten die Ergebnisse einer Studie aus Großbritannien (2021) helfen, die analysiert, wie sehr der Zugang von Betroffenen des Menschenhandels zu Smartphones ein ausschlaggebender Faktor für ihr mentales Wohlbefinden, psychische Gesundheit, Autonomie und Sicherheitsempfinden ist.[156]

152 Eine solche Forderung führt auch die Inter-Agency Coordination Group against Trafficking in Persons (ICAT) in ihrem Statement »Use and abuse of technology« auf, World Day against Trafficking in Persons, 30. Juli 2022.

153 Siehe KOK-Forderungskatalog zur Bundestagswahl 2021, S. 5.

154 BMI, Juni 2022: Cybersicherheitsagenda.

155 bff-Pressemitteilung: InterAktion: Modellprojekt gegen digitale Gewalt startet: Vernetzung von Beratung und IT, 23.03.2022.

156 Unseen UK/BT, Mai 2021. Evaluation report. Impact of mobile technology for survivors of modern slavery and human trafficking: A mixed method study.

AUSBLICK

Menschenhandel wird allgemeinhin als das drittgrößte organisierte Verbrechen betrachtet, nach dem Handel mit Drogen und Waffen. Hat seine Bekämpfung also auch die drittgrößte staatliche Priorität, wenn es um die Verteilung von Ressourcen zur Bekämpfung dieser Verbrechen geht? Bisher sicherlich nicht. Wo Fortschritte in der Verhütung und Bekämpfung des Menschenhandels bisher schon nur mühsam erzielt werden konnten, besteht nun mit zunehmender Entwicklung und verstärktem Einsatz von Informations- und Kommunikationstechnologien durch Menschenhändler*innen die Gefahr, dass sich der Abstand in diesem Rennen vergrößert – auf Kosten der Betroffenen.

Die Digitalisierung des Menschenhandels ist ein Thema, das gekommen ist, um zu bleiben. Es besteht dringender Handlungsbedarf in Deutschland, die Digitalisierung von Behörden vorwärtszubringen, Wissen und Kapazitäten auszubauen und dem komplexen Charakter des Verbrechens, nun mehr denn je, endlich gerecht zu werden, indem eine bessere Zusammenarbeit zwischen Abteilungen, Behörden und Staaten etabliert und strukturell verankert wird. Einzelne Ansätze aus dem internationalen und deutschen Kontext weisen bereits in die richtige Richtung, doch alle Bemühungen und Maßnahmen müssen schneller werden. Dass eine zeitnahe, abgestimmte Reaktion der internationalen Gemeinschaft auf akute Situationen möglich ist, beweisen die Maßnahmen unter der Leitung der EU-Koordinatorin gegen Menschenhandel im Zuge des Ukrainekrieges.[157] Es bleibt zu hoffen, dass Staaten aus dieser Erfahrung lernen und die daraus gewonnenen Erkenntnisse auf ihre Bemühungen um den Schutz aller Betroffenengruppen und die Bekämpfung aller Ausbeutungsformen des Menschenhandels übertragen, im Kontinuum zwischen digital und analog.

157 EU-Kommission, 2022. A Common Anti-Trafficking Plan to address the risks of trafficking in human beings and support potential victims among those fleeing the war in Ukraine – Under the lead of the EU Anti-trafficking Coordinator.

ANHANG

INTERVIEWÜBERSICHT

Nr.	Funktion	Institution	Datum	Art
1	Kriminalhauptkommissarin	BKA SO41	05.07.2022	Telefonisch
2	Beraterin	Jadwiga München	06.07.2022	Telefonisch
3	Beraterin	Dortmunder Mitternachtsmission	11.07.2022	Persönlich
4	Referent	Organisation für Sicherheit und Zusammenarbeit in Europa, Abteilung Menschenhandel und Technologien	12.07.2022	Zoom
5	Referentin	bff – Frauen gegen Gewalt e. V.	14.07.2022	Teams
6	Beraterin	IN VIA Berlin-Brandenburg	15.07.2022	Zoom
7	Beraterin	Fraueninformationszentrum – FIZ Stuttgart	18.07.2022	Teams
8	Staatsanwältin	Staatsanwaltschaft Berlin, Abteilung 255 OK	16.08.2022	Persönlich
9	Beraterin	Fraueninformationszentrum – FIZ Stuttgart	24.08.2022	Telefonisch
10	Zwei IT-forensische Analysten und Gutachter	Forensik.IT GmbH	01.09.2022	Persönlich

LITERATURVERZEICHNIS

- Anti-Trafficking-Review Ausgabe 14, 2020: Special Issue – Technology, Anti-Trafficking, and Speculative Futures. https://www.antitraffickingreview.org/index.php/atrjournal/issue/view/22.

- ARD-Dokumentation: Illegale Prostitution – Das gefährliche Geschäft mit dem Sex, 09.02.2022. https://www.ardmediathek.de/video/betrifft/illegale-prostitution-in-der-pandemie/swr/Y3JpZDovL3N3ci5kZS9hZXgvbzE2MTAxMzQ

- bff e. V., Pressemitteilung InterAktion: Modellprojekt gegen digitale Gewalt startet: Vernetzung von Beratung und IT, 23.03.2022. https://www.frauen-gegen-gewalt.de/de/ueber-uns/presse/pressemitteilungen/pm/pressemitteilung-interaktion-modellprojekt-gegen-digitale-gewalt-startet-vernetzung-von-beratung-und-it.html?fbclid=IwAR1Icu7ggosp4blnVfw8eJihvqPYVa9GfpXAs5-M9P1f2At62BGKUu3DoWA

- bff e. V., 2021: Stellungnahme zum Referentenentwurf eines Gesetzes zur Änderung des Strafgesetzbuches – effektivere Bekämpfung von Nachstellungen und bessere Erfassung des Cyberstalkings. https://www.frauen-gegen-gewalt.de/de/stellungnahmen-1718/stellungnahme-zum-referentenentwurf-eines-gesetzes-zur-änderung-des-strafgesetzbuches-effektivere-bekämpfung-von-nachstellungen.html

- Bracket Foundation, 2022: Gaming and the Metaverse. The Alarming Rise of Online Sexual Exploitation and Abuse of Children Within the New Digital Frontier. https://static1.squarespace.com/static/5d7cd3b6974889646fce45c1/t/632f3344eacdbb108c8c356f/1664037701806/metaverse+%26+gaming.pdf

- Bundesamt für Sicherheit in der Informationstechnik (BSI): Blockchain & Kryptowährung. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Technologien_sicher_gestalten/Blockchain-Kryptowaehrung/blockchain-kryptowaehrung_node.html

- Bundesamt für Sicherheit in der Informationstechnik (BSI): Methoden der Cyber-Kriminalität. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/methoden-der-cyber-kriminalitaet_node.html

- Bundeskriminalamt (BKA):
  - Bundeslagebild Menschenhandel 2021.
  - https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Menschenhandel/menschenhandelBundeslagebild2021.html?nn=27956
  - Bundeslagebild Menschenhandel 2020. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Menschenhandel/menschenhandelBundeslagebild2020.html?nn=27956
  - Bundeslagebild Cybercrime 2021. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2021.html?nn=28110

- Bundesministerium der Justiz (BMJ): Gesetzgebungsverfahren, 17. August 2021. Gesetz zur Änderung des Strafgesetzbuches – effektivere Bekämpfung von Nachstellungen und bessere Erfassung des Cyberstalkings. https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/DE/Cyberstalking.html;jsessionid=A9191AD8E2915A07DA69F46A4CF1FE5D.1_cid334?nn=6704238

- Bundesministerium des Innern und für Heimat (BMI), Juni 2022: Cybersicherheitsagenda. https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/cybersicherheitsagenda-20-legislatur.html

- Bundesregierung:
  - Digitalstrategie. https://digitalstrategie-deutschland.de/ueber-die-digitalstrategie/
  - Mehr Schutz vor sexueller Gewalt, Mitteilung vom 10.11.2016. https://www.bundesregierung.de/breg-de/aktuelles/mehr-schutz-vor-sexueller-gewalt-393682

- Bundesverband der Deutschen Wirtschaft (BVDW): Digital Services Act/Digital Markets Act. https://www.bvdw.org/themen/digitalpolitik/digital-services-actdigital-markets-act/#c10639

- Bundesweiter Koordinierungskreis gegen Menschenhandel – KOK e. V.:
  - 2020: Defining the Gap: Datenerhebung zu Menschenhandel und Ausbeutung in Deutschland – der zivilgesellschaftliche Ansatz des KOK. https://www.kok-gegen-menschenhandel.de/fileadmin/user_upload/KOK_Datenbericht_Final_deu_2020_10_18.pdf
  - Forderungskatalog zur Bundestagswahl 2021. https://www.kok-gegen-menschenhandel.de/fileadmin/user_upload/KOK_Forderungskatalog2021_final.pdf
  - Projektwebseite datACT: https://www.kok-gegen-menschenhandel.de/datenschutz-datact
  - Rechtsprechungsdatenbank. LG Aachen, Urteil vom 25.9.2019, Aktenzeichen 62 KLs 4/19. Schwerer Menschenhandel nach der Loverboy-Methode, Kontaktanbahnung über Internetplattformen

- Bundeszentrale für politische Bildung: Der Arabische Frühling und seine Folgen. https://www.bpb.de/shop/zeitschriften/izpb/238933/der-arabische-fruehling-und-seine-folgen/

- Council of the Baltic Sea States, Task Force against Trafficking in Human beings, 2019: Human Trafficking Glossary. https://cbss.org/publications/human-trafficking-glossary/

- Deutscher Bundestag:
  - Drucksache 19/16763, 19. Wahlperiode, 20.01.2020. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE – Drucksache 19/16101 – Nutzung des Hawala-Systems durch organisierte Kriminalität und terroristische Gruppierungen. https://dserver.bundestag.de/btd/19/167/1916763.pdf
  - Kurzinformation: Die Budapest-Konvention (Cybercrime-Convention) – Aktueller Stand der Verhandlungen zum Zweiten Zusatzprotokoll des Europarates. https://www.bundestag.de/resource/blob/897388/acdeb1ef515226e-0308a2be9c022d328/WD-2-115-20-pdf-data.pdf

- Deutschlandfunk Kultur: Die Bilanz fällt ernüchternd aus, 07.12.2021. https://www.deutschlandfunkkultur.de/reform-des-sexualstrafrechts-bilanz-nach-fuenf-jahren-100.html.

- ECPAT Deutschland e. V. und International Justice Mission Deutschland e. V.: Interdisziplinäres Fachgespräch zur sexuellen Ausbeutung von Kindern per Livestream, Mai 2022. https://ijm-deutschland.de/stop-streaming-exploitation

- ECPAT International:
  - 2019: Explanatory Report to the Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography. https://ecpat.org/resource/opsc-explanatory-reports/
  - 2018: Terminologischer Leitfaden für den Schutz von Kindern vor sexueller Ausbeutung und sexualisierter Gewalt. https://www.terminologie.ecpat.de/wp-content/uploads/2019/12/Terminologischer-Leitfaden-A4-DE.pdf

- Europäische Kommission:
  - 2019: E-evidence – cross-border access to electronic evidence. https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en
  - 2020: Study on the economic, social and human costs of trafficking in human beings within the EU. https://op.europa.eu/de/publication-detail/-/publication/373138c5-0ea4-11eb-bc07-01aa75ed71a1/language-en
  - 2022: A Common Anti-Trafficking Plan to address the risks of trafficking in human beings and support potential victims among those fleeing the war in Ukraine – Under the lead of the EU Anti-trafficking Coordinator. https://home-affairs.ec.europa.eu/system/files/2022-05/Anti-Trafficking%20Plan_en.pdf
  - BERICHT DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT. Dritter Bericht über die Fortschritte bei der Bekämpfung des Menschenhandels (2020) gemäß Artikel 20 der Richtlinie 2011/36/EU zur Verhütung und Bekämpfung des Menschenhandels und zum Schutz seiner Opfer, COM(2020) 661 final vom 20.10.2020. https://ec.europa.eu/transparency/documents-register/api/files/COM(2020)661_0/de00000000994711?rendition=false
  - COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS – A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+), COM(2022) 212 final, 11.5.2022. https://digital-strategy.ec.europa.eu/en/library/digital-decade-children-and-youth-new-european-strategy-better-internet-kids-bik
  - EU-Fahrplan für die Umsetzung der Europäischen Strategie gegen Organisierte Kriminalität, Roadmap – Ares(2021)1264557. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12735-Fighting-organised-crime-EU-strategy-for-2021-25_en
  - Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. Die Strategie der EU zur Bekämpfung des Menschenhandels 2021–2025, COM(2021) 171 final, 14.4.2022. https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52021DC0171&from=EN

  - MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN – EU-Kinderrechtsstrategie, COM(2021) 142 final, 24.03.2021. https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52021DC0142&from=en
  - MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN – EU-Strategie für eine wirksamere Bekämpfung des sexuellen Missbrauchs von Kindern. https://db.eurocrim.org/db/de/doc/3511.pdf
  - Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über eine EU-Strategie zur Bekämpfung der organisierten Kriminalität 2021–2025, COM/2021/170 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021DC0170&qid=1632306192409
  - Mitteilung der Kommission »Gewährleistung der EU-weiten Rechtspflege – Eine Strategie für die justizielle Aus- und Fortbildung auf europäischer Ebene für den Zeitraum 2021–2024«, COM(2020) 713 final vom 2.12.2020.
  - Pressemitteilung vom 23.04.2022. Gesetz über digitale Dienste: Kommission begrüßt politische Einigung über Vorschriften zur Gewährleistung eines sicheren und verantwortungsvollen Online-Umfelds. https://ec.europa.eu/commission/presscorner/detail/de/ip_22_2545; https://rm.coe.int/iris-special-2021-01en-dsa-package/1680a43e45
  - Pressemitteilung, 05.07.2022. Paket zu digitalen Diensten: Kommission begrüßt Annahme des neuen EU-Regelwerks für digitale Dienste durch das Europäische Parlament. https://ec.europa.eu/commission/presscorner/detail/de/ip_22_4313
  - VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&from=DE

- Europäisches Parlament:
  - European Parliamentary Research Service, 2021: Combating gender-based violence: Cyber violence. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662621/EPRS_STU(2021)662621_EN.pdf
  - Legislative Entschließung des Europäischen Parlaments vom 5. Juli 2022 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über bestreitbare und faire Märkte im digitalen Sektor (Gesetz über digitale Märkte) (COM(2020)0842 – C9-0419/2020 – 2020/0374(COD)). https://www.europarl.europa.eu/doceo/document/TA-9-2022-0270_DE.html
  - Legislative Entschließung des Europäischen Parlaments vom 5. Juli 2022 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über einen Binnenmarkt für digitale Dienste (Gesetz über digitale Dienste) und zur Änderung der Richtlinie 2000/31/EG (COM(2020)0825 – C9-0418/2020 – 2020/0361(COD)). https://www.europarl.europa.eu/doceo/document/TA-9-2022-0269_DE.html#title1

  - Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt (»Richtlinie über den elektronischen Geschäftsverkehr«). https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32000L0031&from=de
  - RICHTLINIE 2011/36/EU DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 5. April 2011 zur Verhütung und Bekämpfung des Menschenhandels und zum Schutz seiner Opfer sowie zur Ersetzung des Rahmenbeschlusses 2002/629/JI des Rates. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:101:0001:0011:DE:PDF
  - Schlussfolgerungen des Rates über die Festlegung der EU-Prioritäten für die Bekämpfung der schweren und organisierten Kriminalität im EMPACT- Zyklus 2022-2025, Brüssel, den 12. Mai 2021 (OR. en), 8665/21. https://data.consilium.europa.eu/doc/document/ST-8665-2021-INIT/de/pdf
  - Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern, COM(2022) 209 final, 2022/0155(COD), 11.05.2022. https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52022PC0209&from=EN

- Europarat:
  - 2011. Explanatory Report to the Council of Europe Convention on preventing and combating Violence Against Women and domestic violence, Council of Europe Treaty Series No. 210. https://docentes.fd.unl.pt/docentes_docs/ma/TQB_MA_32409.pdf
  - 2021. Protecting women and girls from violence in the digital age. The relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in addressing online and technology-facilitated violence against women. https://rm.coe.int/prems-153621-gbr-2574-study-online-a4-bat-web/1680a4cc44
  - 2022. Online and technology-facilitated trafficking in human beings. https://rm.coe.int/online-and-technology-facilitated-trafficking-in-human-beings-full-rep/1680a73e49new-report-on-online-and-technology-facilitated-trafficking-in-human-beings
  - Cybercrime Convention Committee (T-CY), Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. Explanatory Report, 17.11.2021. https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4b
    Zweites Zusatzprotokoll zum Übereinkommen über Computerkriminalität betreffend die Verstärkung der Zusammenarbeit und der Weitergabe von elektronischem Beweismaterial, 12.05.2022. https://rm.coe.int/1680a6f604.

- EUROPOL
  - 2022: European Migrant Smuggling Center. 6th Annual Report. https://www.europol.europa.eu/cms/sites/default/files/documents/EMSC%206%20th%20Annual%20Report.pdf
  - 2020: The challenges of countering human trafficking in the digital era. https://www.europol.europa.eu/cms/sites/default/files/documents/the_challenges_of_countering_human_trafficking_in_the_digital_era.pdf

- Fuß, M., 2020: Forensische Linguistik – Sprachanalyse in Darknet-Foren zu sexuellem Missbrauch und Ausbeutung von Kindern. https://dpt-statisch.s3.eu-central-1.amazonaws.com/dpt-digital/dpt-25/medien/dateien/454/2020_Darknet_Sprachanalyse_ECPAT-kurz.pdf

- Initiative D21 e. V./Kompetenzzentrum Technik-Diversity-Chancengleichheit e. V., 2020: Digital Gender Gap. Lagebild zu Gender(un)gleichheiten in der digitalisierten Welt. https://www.kompetenzz.de/aktivitaeten/digital-gender-gap

- Inter-Agency Coordination Group against Trafficking in Persons (ICAT):
  - Human Trafficking and Technology: Trends, Challenges and Opportunities. Issue Brief 7/2019. https://icat.un.org/sites/g/files/tmzbdl461/files/human_trafficking_and_technology_trends_challenges_and_opportunities_web.pdf
  - Statement: Use and Abuse of Technology, World Day against Trafficking in Persons, 30. Juli 2022. https://icat.un.org/sites/g/files/tmzbdl461/files/publications/icat_statement_wdat_2022.pdf

- Kinderrechte.digital – ALLGEMEINE BEMERKUNG Nr. 25 (2021) Über die Rechte der Kinder im digitalen Umfeld: https://kinderrechte.digital/hintergrund/index.cfm/topic.280/key.1738.

- Kommuniqué der G7-Staats- und Regierungschefs, 28.06.2022. https://www.consilium.europa.eu/media/57555/2022-06-28-leaders-communique-data.pdf

- Kramer, F., 2020: Mit THB Liberi organisierten Menschenhandel bekämpfen.
  In: Die Polizei, 11-2020

- Milivojevic, S./Moore, H./Segrave, M.: Freeing the Modern Slaves, One Click at a Time: Theorising human trafficking, modern slavery, and technology. In: Anti-Trafficking Review, Ausgabe 14, 2020, S. 16–32. https://www.antitraffickingreview.org/index.php/atrjournal/article/view/442/351

- Muffet, Alec: Real World Onion Sites, 2022. https://github.com/alecmuffett/real-world-onion-sites/blob/master/master.csv

- Organization for Security and Co-operation in Europe (OSCE)
  - 2022: Recommendations on enhancing efforts to identify and mitigate risks of trafficking in human beings online as a result of the humanitarian crisis in Ukraine. https://www.osce.org/cthb/516423
  - 2020: Leveraging innovation to fight trafficking in human beings: a comprehensive analysis of technology tools. https://www.osce.org/secretariat/455206
  - Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings, 2022: Policy Responses to Technology-Facilitated Trafficking in Human Beings: Analysis of Current Approaches and Considerations for Moving Forward. https://www.osce.org/files/f/documents/0/d/514141.pdf

- Pacific Links Foundation: PAXU. https://pacificlinks.org/paxu/#Courage.

- Phillips, K./Davidson, J. C./Farr, R. R./Burkhardt, C./Caneppele, S./Aiken, M. P.: Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. In: Forensic Sciences 2022, 2, 379–398

- Polaris, 2018: On-Ramps, Intersections, and Exit Routes: A Roadmap for Systems and Industries to Prevent and Disrupt Human Trafficking. https://polarisproject.org/wp-content/uploads/2018/08/A-Roadmap-for-Systems-and-Industries-to-Prevent-and-Disrupt-Human-Trafficking.pdf.

- Raets, S./Janssens, J., 2019. Trafficking and Technology: Exploring the Role of Digital Communication Technologies in the Belgian Human Trafficking Business. In: European Journal on Criminal Policy and Research (2021) 27, S. 15–238. https://link.springer.com/article/10.1007/s10610-019-09429-z

- Reid, R./Fox, B., 2020: Human Trafficking and the Darknet: Technology, Innovation, and Evolving Criminal Justice Strategies. https://link.springer.com/chapter/10.1007/978-3-030-41287-6_5

- Rüdiger, T., 2017: Das Broken-Web-Phänomen. In: Jur@ im Netz. https://www.researchgate.net/publication/320490473_Das_Broken-Web-Phanomen_-_Jur_im_Netz

- Statista.de: Anteil der Internetnutzer in ausgewählten Ländern in Europa im Jahr 2021: https://de.statista.com/statistik/daten/studie/184636/umfrage/internetreichweite-anteil-der-nutzer-in-europa/

- Statista.de: Statistiken zur Internetnutzung weltweit: https://de.statista.com/themen/42/internet/#dossierKeyfigures

- Stop The Traffik, 2018: Human Trafficking and the Darknet: Insights on supply and demand. https://www.stopthetraffik.org/wp-content/uploads/2019/06/Human-Trafficking-and-the-Darknet-Insights-FINAL-1.pdf.
- Tamm, A./Volbert, R., Präsentation vom 10.05.2022: Das Projekt ViContact. Befragungen bei Verdacht auf sexuellen Missbrauch – Training in virtueller Umgebung

- Teschner, G.: Sex on Demand. Prostitution geht online, Menschenhandel und Ausbeutung auch? In: Kriminalistik 11/2021, S. 645–648

- UNICEF, 2022 – Legislating for a digital age, Glossary. https://www.childrenrights.de/content/user_upload/UNICEF__BMZ__GIZ__2022._Summary_Legislating_for_the_digital_age_.pdf

- United Nations Office on Drugs and Crime (UNODC), 2021: The effects of the Covid19 pandemic on trafficking in persons and responses to the challenges. https://www.unodc.org/documents/human-trafficking/2021/The_effects_of_the_COVID-19_pandemic_on_trafficking_in_persons.pdf

- Unseen UK/BT, May 2021. Evaluation report. Impact of mobile technology for survivors of modern slavery and human trafficking: A mixed method study. https://www.unseenuk.org/wp-content/uploads/2021/10/FINAL-Unseen-BT-Evaluation-report_Technology-report_17MAY.pdf

- Wall, D. S., 2017: Crime, security and information communication technologies: The changing cybersecurity threat landscape and implications for regulation and policing. In: Brownsword, R./Scotford, E./Yeung, K. (Hrsg.): The Oxford Handbook on the Law and Regulation of Technology, o. S. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3005872

- WeProtect Global Alliance, 2021: Framing Child Sexual Abuse and Exploitation Online as a Form of Human Trafficking: Opportunities, Challenges and Implications. Expert Roundtable Outcomes Briefing. https://www.weprotect.org/wp-content/uploads/WeProtect-Global-Alliance-Trafficking-Roundtable-Outcomes-Briefing-2021.pdf

IMPRESSUM

MENSCHENHANDEL 2.0 –
DIGITALISIERUNG DES MENSCHENHANDELS
IN DEUTSCHLAND
Entwicklungen und Handlungsoptionen

Herausgeber:
Bundesweiter Koordinierungskreis gegen Menschenhandel – KOK e. V.
Lützowstr. 102–104 / Hof 1, Aufgang A
10785 Berlin
Telefon: (+49) 030 / 263 911 76
Fax: (+49) 030 / 263 911 86
info@kok-buero.de
www.kok-gegen-menschenhandel.de

Autorin: Dr. Dorothea Czarnecki
Lektorat / Korrektorat: Ulrike Gatzke
Grafische Gestaltung und Satz: Ricarda Löser, Weimar
Titelbild: istockphoto.com/royyimzy
V. i. S. d. P.: Sophia Wirsching
Druck: hinkelsteindruck, Berlin
Auflage: 300 Exemplare

Bankverbindung:
KOK e. V.
Evangelische Bank eG
IBAN: DE43 5206 0410 0003 9110 47
BIC: GENODEF1EK1

ISBN: 978-3-9821936-8-7

Der KOK e. V. wird gefördert vom:

Bundesministerium
für Familie, Senioren, Frauen
und Jugend

KOK
Bundesweiter Koordinierungskreis
gegen Menschenhandel e.V.

Lützowstr. 102 – 104 I Hof 1, Aufgang A
10785 Berlin
Telefon: (+49) 030 / 263 911 76
Fax: (+49) 030 / 263 911 86
info@kok-buero.de
www.kok-gegen-menschenhandel.de

9 783982 193687