Zur Datafizierung von Intimität und strafrechtsrelevanten, datenbasierten Zugriffen auf die sexuelle Selbstbestimmung

– Von sogenanntem Image-Based Sexual Abuse (IBSA) zum Data-Based Sexual Abuse (DBSA) –

Von Prof. Dr. Liane Wörner, LL.M. (UW-Madison) / Wiss. Ass. Lena Gmelin*

„Revenge Porn", „Upskirting" und „Deep Fakes" sind Beispiele für Phänomene, die derzeit unter dem bereits etablierten Oberbegriff „image-based sexual abuse" (IBSA, dt. bildbasierter sexueller Missbrauch) zusammengefasst werden. Die eigentliche Gefahr liegt jedoch nicht allein in der Verwendung bildlicher Darstellungen zur Bloßstellung, Erpressung oder Ausübung sexueller Gewalt gegenüber Betroffenen, sondern in der fortschreitenden Datafizierung menschlicher Kommunikation (einschließlich der sexuellen Kommunikation) und den sich daraus ergebenden, weit über die Bildverwendung hinausweisenden, Missbrauchsmöglichkeiten. Es soll hier daher von vornherein das übergeordnete Phänomen als „datenbasierte sexuelle Gewalt" anhand von drei zentralen Elementen analysiert werden: (1) die Nicht-Einvernehmlichkeit auf einer oder mehreren Handlungsebenen, (2) eine sexuelle Konnotation und (3) die Ausführung einer oder mehrerer Ebenen mittels digitaler Technologie. Die Analyse des deutschen Strafrechts aus völkerrechtlicher Perspektive zeigt erhebliche materiellrechtliche Lücken in der Strafbarkeit sowie praktische Herausforderungen bei der Strafverfolgung auf. Insbesondere im Hin-

* Prof. Dr. Liane Wörner, LL.M. (UW-Madison) ist Professorin für Strafrecht, Strafprozessrecht, Vergleichendes Strafrecht, Medizinisches Strafrecht und Rechtstheorie sowie Direktorin des Zentrums für Mensch | Daten | Gesellschaft an der Universität Konstanz, Deutschland. Lena Gmelin ist wissenschaftliche Mitarbeiterin am Lehrstuhl von Prof. Dr. Liane Wörner, LL.M. (UW-Madison). Ein gemeinsamer Beitrag in englischer Sprache ist 2024 erschienen in RIDP 95 (2) 2024, S. 367–390; dieser Beitrag setzt die dort angestellten Überlegungen fort und berücksichtigt die deutsche Diskussion.

RW 3/2025, DOI: 10.5771/1868-8098-2025-3-239

blick auf KI-generierte Inhalte ist der deutsche Gesetzgeber aufgefordert, zeitnah Regelungen zu schaffen. Hierfür kann aber, und das zeigt der Beitrag, der bestehende Straftatbestand der Urkundenfälschung (§ 267 StGB) als Blaupause dienen.

A. Einleitung: Von bildbasierten zu datenbasierten sexuellen Übergriffen – ein umfassenderer Ansatz zur Definition des Phänomens

Wie nahezu jede andere Form zwischenmenschlicher Kommunikation und Interaktion wird auch die menschliche Sexualität nicht von der Datafizierung verschont. Im Gegenteil, die Erotikfilmindustrie kann als eine der treibenden Kräfte für bestimmte technologische Fortschritte bezeichnet werden.[1] Die durch das Internet geschaffenen anonymen und niedrigschwelligen Möglichkeiten der sexuellen Kommunikation, Erkundung und Ausbeutung – sei es offen zugänglich oder in verborgenen Darknet-Foren –, sind ein regelrechter Nährboden für weit mehr als nur moderne Sexualaufklärung und Emanzipation.[2] Taten, die früher ausschließlich in den intimsten und privatesten Bereichen menschlicher Interaktion stattfanden, werden plötzlich in den öffentlichsten und zugänglichsten aller Räume verlagert – das Internet. Das breite Spektrum sozial unerwünschter sexueller Kommunikationshandlungen reicht von (noch) nicht strafbar bis strafrechtlich hochrelevant, von alltäglichen, normalisierten und akzeptierten Verhaltensweisen bis hin zu solchen, die zur Einrichtung spezieller Bundesverfolgungsbehörden und zur Gründung von Bürgerinitiativen geführt haben. Bildbasierte sexuelle Kommunikation kann vielfältige Formen annehmen, von denen nur einige einvernehmlich sind. Diejenigen, die nicht einvernehmlich sind, stellen bildbasierte sexuelle *Gewalt*[3] (*image-based sexual abuse*, IBSA) dar.

IBSA gilt dabei als ein relativ neues Phänomen, dessen Ausprägungen jedoch eine erhebliche und geschlechtsspezifische Bedrohung für die sexuelle und informationelle Selbstbestimmung darstellen. Dennoch machen soziale und gesellschaftspolitische Bewegungen sowie legislative Bemühungen die Defizite in Prävention, Kriminalisierung und effektiver Strafverfolgung von IBSA deutlich. Rechtsordnungen sind (weitenteils) noch nicht für die Bekämpfung digitaler Straftaten gerüstet. Der schnelle technologische Fortschritt vergrößert sekündlich den digitalen Raum, gestaltet ihn komplexer und erweitert das Spektrum möglicher Straftaten erheblich.

1 *M. Hall/J. Hearn/R. Lewis*, Image-Based Sexual Abuse: Online Gender-Sexual Violations, 3 Encyclopedia 2023, S. 327 (327 f.) beschreiben die „long histories of the relationship between sex, sexuality and technologies" (dt.: „lange Geschichte der Beziehung zwischen Sex, Sexualität und Technologien").

2 Vgl. auch *J.-K. Bauer/A. Hartmann*, Formen digitaler geschlechtsspezifischer Gewalt, in: bff: Bundesverband Frauenberatungsstellen und Frauennotrufe/N. Prasad (Hrsg.), Geschlechtsspezifische Gewalt in Zeiten der Digitalisierung – Formen und Interventionsstrategien, Bielefeld 2021, S. 63 (63 ff.).

3 Vgl. zum Begriff der bildbasierten sexualisierten *Gewalt* in Gegenüberstellung zum übersetzten „abuse" als „Missbrauch" *R. Sanow*, Die Strafbarkeit voyeuristischer Bildaufnahmen, Baden-Baden 2025, S. 56 ff.

Dies stellt die Rechtssysteme vor große Herausforderungen und erschwert die Implementierung zeitgemäßer staatlicher Schutzmechanismen auf allen Ebenen, insbesondere auf der legislativen. Aufgrund, selbst komplexer, träger sozialer und politischer Entscheidungsprozesse und notwendigerweise langwieriger Gesetzgebungsverfahren können Rechtssysteme kaum mit dem Tempo der digitalen Innovation Schritt halten. Mit der Einführung des § 184k StGB[4] im Jahr 2020, der die Verletzung des Intimbereichs durch die Herstellung, die Übertragung, den Gebrauch oder das Zugänglichmachen von Bildaufnahmen intimer Körperteile unter Strafe stellt, hat der deutsche Gesetzgeber einen bedeutenden ersten Schritt in Richtung eines besseren Schutzes vor bestimmten Arten von IBSA getan.

Es gilt damit, das Phänomen des IBSA zu definieren und im weiteren Kontext der deutschen (Straf-)Rechtswissenschaft und -dogmatik zu untersuchen. Während schon der Begriff des „sexuellen Missbrauchs" bzw., für den vorliegenden Kontext vorzugswürdig, der „sexuellen Gewalt" umstritten ist, weil unklar bleibt, welche Verhaltensweisen umfasst sind, ist der Begriff der „bildbasierten sexuellen Gewalt" noch recht neu und in seiner Definition und Abgrenzung noch schwieriger zu (er)fassen. Fasst man die bisher vorgelegten Vorschläge zusammen, erscheinen drei Elemente maßgebend, um ein Verhalten als IBSA einzuordnen: (1) das fehlende Einverständnis der betroffenen Person, (2) die Weitergabe von Bildern oder Videos und (3) der sexuell explizite oder sexuell konnotierte Charakter des Materials; wobei irrelevant bleibt, ob die Weitergabe offline oder online erfolgt oder ob das Bildmaterial „echt" oder „gefälscht" ist.[5] An anderer Stelle ist auch komplexer vom „mehrdimensionalen Konstrukt" die Rede,[6] das über die reine Weitergabe von Bildern hinausgeht und auch andere Verhaltensweisen umfasst, darunter das nicht-einvernehmliche Aufnehmen von Nackt- oder Sexualaufnahmen[7] und/oder bereits die Androhung, solches Material zu verbreiten.[8]

IBSA wird dabei im Allgemeinen als Oberbegriff verwendet. Die verschiedenen Vorschläge versuchen jeweils den Bedeutungsgehalt des Begriffs insgesamt dadurch zu erfassen, dass denkbare Verhaltensweisen beschrieben werden.[9] Diese reichen von der bloßen Verbreitung über die Herstellung bis hin zur Nutzung von Bildma-

4 Die Bestimmung wurde durch das 59. StrÄndG vom 9.10.2020 (BGBl. I S. 2075) ergänzt und trat am 1.1.2021 in Kraft.

5 *Hall/Hearn/Lewis*, IBSA (Fn. 1), S. 327.

6 *M. Paradiso/L. Rollè/T. Trombetta*, Image-Based Sexual Abuse Associated Factors: A Systematic Review, Journal of family violence 2023, S. 1 (1 f.).

7 *C. McGlynn/K. Johnson/E. Rackley/N. Henry/N. Gavey/A. Flynn/A. Powell*, „It's Torture for the Soul": The Harms of Image-Based Sexual Abuse Social & legal studies 2021, S. 541.

8 *Paradiso/Rollè/Trombetta*, IBSA-Associated Factors (Fn. 6), S. 12 f.

9 Vgl. z.B. *D. Fido/C. Harper*, Non-Consensual Image-Based Sexual Offending, Cham, Palgrave Macmillan/Springer Nature 2020, S. 3, die IBSA als einen weit gefassten Rechtsbegriff betrachten, der eine „Sammlung von Verhaltensweisen" beschreibt.

terialien als Nötigungsmittel. Viele der zur Beschreibung von IBSA herangezogenen Verhaltensweisen sind selbst eher neue Phänomene. Zwar ist es notwendig, die Bandbreite der Verhaltensweisen zu kennen, die von einer Definition abgedeckt werden sollen, doch enden viele Definitionsversuche an dieser Stelle und konzentrieren sich – insoweit nicht abschließend – auf einzelne Erscheinungsformen.[10] In der Folge variiert die Bedeutung des Begriffs und unterliegt einem stetigen Wandel; fortlaufend treten neue Arten missbräuchlichen Verhaltens hinzu. Weitgehender Konsens besteht allein hinsichtlich der grundsätzlichen Schädlichkeit von IBSA.

Eine Studie von *McGlynn et al.*[11] hat fünf wesentliche Schadensdimensionen identifiziert: soziale Entfremdung,[12] Gefühle der Konstanz (die „Endlosigkeit" der erlittenen Schäden)[13] und der existenziellen Bedrohung,[14] Isolation[15] und eingeschränkte Handlungsfreiheit.[16] Diese Schadensfaktoren machen deutlich, dass ein wirksames und umfassendes Präventions- und Schutzkonzept erforderlich ist. Die uneinheitlichen Definitionsansätze erschweren jedoch die wissenschaftliche Erfassung des Phänomens.

Darüber hinaus gibt es Verhaltensweisen, die durch den Begriff *bild*basierter sexueller Gewalt nicht ausdrücklich erfasst werden, aber in vielerlei Hinsicht mit IBSA vergleichbar sind: so haben einige, derzeit als IBSA bewertete Phänotypen einen anderen Schwerpunkt als das dabei verwendete Bildmaterial (z.B. bildbasierte sexuelle Erpressung[17] oder Phishing sexuell konnotierter oder sexualisierter Daten). Einige Arten sexueller Gewalt sind nicht bildbasiert, wohl aber *daten*basiert und weisen vergleichbare Risiken und Folgen auf. Unklar ist etwa, weshalb die nicht-einvernehmliche Verbreitung einer visuellen pornografischen Aufzeichnung IBSA sein soll, nicht aber die nicht-einvernehmliche Verbreitung einer sexuellen Audioaufzeichnung mit wiedererkennbarer Stimme.[18] Trotz unterschiedlicher Iden-

10 Vgl. *C. McGlynn/E. Rackley/R. Houghton*, Beyond ‚Revenge Porn': The Continuum of Image-Based Sexual Abuse 5 Feminist Legal Studies 2017, S. 25 (28); *J. Blocher*, Strafbare Deepfakes als Täuschung über die Authentizität von Medieninhalten. „Ich traue meinen Augen kaum", KIR 2025, S. 225 (228), die ebenfalls das Problem erkennen, den Fokus (nur) auf Einzelphänomene zu legen.

11 *McGlynn/Johnson/Rackley/Henry/Gavey/Flynn/Powell*, Harms of IBSA (Fn. 7).

12 Ebd., S. 550 ff. beschreiben auch die weiteren Folgen wie das potenzielle Risiko der Stigmatisierung, Beschämung oder gar ehrbezogener Gewalt.

13 Ebd., S. 552.

14 Ebd., S. 553.

15 Ebd., S. 554 f.

16 Ebd., S. 555 ff.; vgl. auch *A. Schmidt*, Pornographie und sexuelle Selbstbestimmung, Tübingen 2025, S. 244 f. m.w.N.

17 *C. McGlynn/E. Rackley*, Image-Based Sexual Abuse, Oxford Journal of Legal Studies 2017, S. 534 (536) m.w.N.

18 Mit der Weiterentwicklung der Datafizierung und einer Vielzahl von Datenformaten entwickeln sich auch die Risiken von Fälschungen und/oder Täuschungen weiter; vgl. auch *N. Klass*, Manipulierte Realität: Wie Deepfakes Recht und Gesellschaft herausfordern, ZUM 2025, S. 485 (485 f.); vgl. zu den Risiken im Zusammenhang mit Deepfake-Stimmmanipulationen ebd., S. 486 f.; *C. Okolie*, Artificial Intelligence-Altered Videos (Deepfakes), Image-Based Sexual Abuse, and Data Privacy Con-

tifizierungsmöglichkeiten kann für visuelle Inhalte sowie Audio- bzw. audiovisuelle Inhalte doch ein vergleichbarer Schutzbedarf bestehen. Das gilt richtigerweise auch für die Erstellung von kinderpornografischen Schriften, „digital catcalling", „doxing"[19] sowie für das seit langem diskutierte Thema sexualisierter Hassrede[20] im Internet.

Nichts anderes zeigt auch der Fall um die Schauspielerin *Collien Fernandes*: Die ihrem Ex-Mann *Christian Ulmen* vorgeworfenen Handlungen beschränken sich bei Weitem nicht auf bildbasierte Kommunikation. Von *Fernandes* waren auf Plattformen (bspw. LinkedIn) Fake-Profile erstellt worden; die dahinterstehende Person hatte sich als *Fernandes* ausgegeben und sich mit Männern zu Telefonaten mit sexuellem Inhalt verabredet.[21] Weiter wurden pornografische Bilder und Videos verschickt, in denen Frauen auftraten, die *Fernandes* täuschend ähnlich sehen, um den Eindruck zu erwecken, sie werde gezeigt; unter den Aufnahmen finden sich auch sexualisierende Deepfakes von *Fernandes*. Die Bild- und Videomaterialien sind freilich ein großer Teil dessen, was die Übergriffigkeit der Handlungen gegenüber *Fernandes* ausmachen. Zugleich ist die von ihr als „virtuelle Vergewaltigung"[22] bezeichnete digitale Gewalt nicht auf visuelle Inhalte beschränkt. Die von *Fernandes* in Spanien erstattete Anzeige beinhaltet verschiedene Delikte, darunter als nicht-körperliche Delikte eine Anmaßung des Personenstands, öffentliche Beleidigung, die Offenlegung von Geheimnissen, schwere Bedrohung; mit eingereicht wurden Fotos und Videos, aber auch E-Mails, Handychats und Audiodateien.[23] Die Handlungen weisen alle sowohl eine sexuelle als auch eine digitale Komponente auf. *Fernandes* spricht davon, im Internet sexuell zur Verfügung gestellt, zum Objekt gemacht worden zu sein.[24] Der Fall zeigt gerade das Ausmaß, das derartige Übergriffe annehmen können, das über bildhafte Inhalte deutlich hinausgeht; es betrifft auch die Kommunikation mit der betroffenen Person, ihre persönliche Darstellung, ihre Identität.

cerns, Journal of International Women's Studies 2023, Artikel Nr. 11, S. 6; *C. Engel-Bunsas*, Recht an der eigenen Stimme in Zeiten von Deepfakes, RDi 2025, S. 292.

19 *S. Andresen*/*S. Dreyer*, Straf- und jugendschutzrechtliche Bewertung von Online-Formen aufgezwungener Sexualität und sexualisierter Belästigung, JMS 2021, S. 2 (2 f.).

20 Hierzu ist im Gesamtkontext auch die geschlechtsspezifisch diskriminierende Radikalisierung in bestimmten Online-Räumen zu nennen, vgl. ausführl. Deutscher Juristinnenbund e.V. (djb), Policy Paper: Netz als antifeministische Radikalisierungsmaschine (st21–18 vom 9.9.2021), online abrufbar unter <https://www.djb.de/presse/stellungnahmen/detail/st21-18>, zuletzt abgerufen am 20.2.2026; vgl. weiter auch *Schmidt*, Pornographie (Fn. 16), S. 296 ff. m.w.N.

21 *L. Eberle*/*R. Höfner*/*M. Hoppenstedt Heinrichs*/*J. Löffler*/*M. Milatz*, „Du hast mich virtuell vergewaltigt". Strafanzeige gegen Christian Ulmen, DER SPIEGEL v. 21.03.2026 (13/2026).

22 Ebd.

23 Ebd. Zu wieder aufgenommenen Ermittlungen in Deutschland zuletzt DIE ZEIT, AFP, Digitale Gewalt:
Ermittlungen im Fall Fernandes in Deutschland wiederaufgenommen v. 27.3.2026 (online-Ausgabe).

24 So ausweislich der Spiegelrecherche, *Eberle*/*Höfner*/*Hoppenstedt Heinrichs*/*Löffler*/*Milatz*, Strafanzeige gegen Christian Ulmen (Fn. 21).

Der Begriff „bildbasiert" setzt einen Adressaten voraus und umfasst einen bestimmten Erwartungshorizont. Daher kann der Begriff IBSA konzeptionell nicht alle Formen sexueller Übergriffe abdecken, die mit den Risikofaktoren datenbasierter Kommunikation zusammenhängen: Die Beschränkung von Formen sexuellen Missbrauchs, die über Daten oder das Internet begangen werden, auf bildbasierte Inhalte grenzt den Begriff zu stark ein und schließt andere, eng verwandte Formen aus. Die Gefahren der Datafizierung – insbesondere im Kontext sexueller Kommunikation – liegen jedoch woanders und müssen ausgehend von der Handlung selbst definiert werden, nicht anhand der Wahrnehmung oder Erscheinungsform. Obwohl sie letztlich weiterhin an die IBSA-Kategorie anknüpfen, verfolgen einige Autor*innen einen weiteren Ansatz, der konkreter auf die eingesetzten Mittel abstellt und die Rolle der Technologisierung ausdrücklich mitberücksichtigt.[25]

Ein neuer Definitionsansatz ist zur Rechts(guts)entwicklung erforderlich. Dabei ist ein überzeugendes Argument für die Erneuerung und Erweiterung der Definition bereits im deutschen Strafrecht verankert: bei einigen Sexualdelikten stellt das deutsche Strafgesetzbuch andere Arten von Inhalten mit bildbasierten Inhalten gleich. Die §§ 184–184c StGB beziehen sich jeweils auf bestimmte Arten pornografischer „Inhalte", nicht auf „Bilder". Der Begriff „Inhalt" ist in § 11 Abs. 3 StGB legaldefiniert; Inhalte sind danach „solche, die in Schriften, auf Ton- oder Bildträgern, in Datenspeichern, Abbildungen oder anderen Verkörperungen enthalten sind oder auch unabhängig von einer Speicherung mittels Informations- oder Kommunikationstechnik übertragen werden".[26] Legen wir diese Definition zugrunde, wird der IBSA-Begriff bereits konzeptionell fortgeführt. Die negativen Folgen, die mit IBSA verbunden sind und die eine gesonderte Analyse des Phänomens erfordern, sind danach offensichtlich nicht auf bildbasierte Daten beschränkt. Letztendlich ist nicht die *Art* der Daten, die als Mittel der sexuellen Gewalt verwendet werden, für die Unterscheidung dieses modernen Phänomens entscheidend, sondern die Tatsache, *dass* eine Datafizierung der sexuellen Kommunikation als Mittel der sexuellen Übergriffigkeit[27] eingesetzt wird. Um diesem Umstand zentral Rechnung

25 Vgl. z.B. *N. Henry/A. Flynn/A. Powell*, Policing image-based sexual abuse: stakeholder perspectives, Police Practice and Research 2018, S. 565 unter Bezugnahme auf den Begriff „technology-facilitated sexual violence" (dt. technologiegestützte sexuelle Gewalt); siehe auch *Hall/Hearn/Lewis*, IBSA (Fn. 1), S. 329, die IBSA als Teil der Technologisierung von Sozialität, Sexualität und Gewalt betrachten und als „Online- und andere technologisch verknüpfte Aktivitäten und Aktivitäten, die anderen Schaden zufügen" beschreiben.

26 Auch die RL (EU) 2024/1385 differenziert – bspw. in Art. 5 Abs. 1 lit. a) – zwischen „Bildern, Videos oder vergleichbarem Material". Erfasst sein sollen nach Erwägung Nr. 19 der Richtlinie „alle Arten von solchem Material", namentlich „Bilder, Fotos und Videos, einschließlich sexualisierter Bilder, Audio- und Videoclips", ebenso KI- oder anderweitig manipulierte Daten.

27 Einen Fokus auf die Wirkung sexualisierter Gewalt im Kontext des Rechtsguts der sexuellen Selbstbestimmung – unabhängig von ihrer nicht-körperlichen Ausprägung – setzen bspw. auch *B. Völzmann*, Deepfake-Pornografie: Schutz durch das Recht auf sexuelle Selbstbestimmung und seine einfachgesetzlichen Ausprägungen, ZUM 2025, S. 493 (497); *B. Burghardt/A. Schmidt/L. Steinl* (zu-

zu tragen, wird hier im Weiteren das Konzept der „datenbasierten sexuellen Gewalt“ (data-based sexual abuse, kurz DBSA) verwendet.

Es gilt also, den Begriff, die verschiedenen Erscheinungsformen und Dimensionen von DBSA und die geschlechtsspezifischen Besonderheiten zu erörtern (B.), die aktuelle Rechtslage auf internationaler und nationaler Ebene darzustellen, um die von DBSA betroffenen Rechtsgüter sowie deren Schutzzwecke zu untersuchen, und ihre strafrechtliche Erfassung für das deutsche Recht zu erfragen (C.). Auf die Notwendigkeit und Ausgestaltung künftiger gesetzgeberischer Maßnahmen gilt es hinzuweisen (D.).

B. Typologie und Grundlagen von DBSA

Nach herrschender Auffassung lassen sich mehrere Verhaltensweisen und Phänomene unter dem Begriff der bildbasierten sexuellen Gewalt zusammenfassen. Die Herstellung pornografischer Bilder durch das Fotografieren oder Filmen einer Person ohne deren Zustimmung wird dabei einheitlich als IBSA verstanden. Hierzu zählen die speziellen Phänomene des „Upskirting” und „Downblousing”, zwei Begriffe, die das nicht-einvernehmliche Fotografieren der Intimbereiche einer Person unter ihrer Oberbekleidung beschreiben[28] (typischerweise durch das Hochfotografieren unter den Rock oder das Hinunterfotografieren in den Ausschnitt). Derartige Praktiken haben sich vor allem mit der Verbreitung von foto- und videofähigen (Smart-)Phones etabliert, die das unbemerkte Aufnehmen von Bildern in öffentlichen, alltäglichen Situationen erheblich erleichtert haben. Die Herstellung pornografischer Bilder ohne Einwilligung umfasst unstreitig auch Formen des digitalen Voyeurismus. Während unter klassischem Voyeurismus hauptsächlich Formen des Beobachtens einer anderen Person in intimen Situationen (z.B. beim Ausziehen, Duschen, bei sexuellen Handlungen usw.) zur Erlangung sexueller Befriedigung[29] verstanden werden, hat der Einsatz digitaler Geräte das Spektrum erheblich erweitert:[30] Es sind weitaus invasivere Formen des Voyeurismus entstanden, etwa durch die Installation versteckter Kameras, um eine Person heimlich zu filmen und die Aufnahmen anschließend anzusehen, zu speichern oder live zu streamen. Das Streaming und Hochladen solcher Bilder hat sich inzwischen zu einer rasch wachsenden, kommerziell ausgerichteten Branche entwickelt, in der pornografisches Material entgeltlich angeboten wird.

gleich Hrsg.), Sexuelle Selbstbestimmung jenseits des Körperlichen. Zur Einführung, im gleichnamigen Sammelwerk, S. 1 f. sowie *Sanow*, Voyeuristische Bildaufnahmen (Fn. 3), S. 73.

28 *McGlynn/Rackley/Houghton*, Continuum of IBSA (Fn. 10), S. 32; *Fido/Harper*, Image-Based Sexual Offending (Fn. 9), S. 9.

29 *McGlynn/Rackley/Houghton*, Continuum of IBSA (Fn. 10), S. 31; *Fido/Harper*, Image-Based Sexual Offending (Fn. 9), S. 9.

30 *McGlynn/Rackley*, IBSA (Fn. 17), S. 38.

IBSA (im engeren Sinne also) umfasst jedoch auch die Verbreitung pornografischer Aufnahmen, die eine Person zeigen, ohne dass diese den dargestellten sexuellen Handlungen, der Herstellung der Aufnahmen und/oder deren Verbreitung zugestimmt hat. Dies äußert sich typischerweise in Form von sog. Rachepornografie (engl. „Revenge Porn"), d.h. der Online-Verbreitung ursprünglich einvernehmlich entstandener sexueller Fotos oder Videos als Racheakt nach Beendigung der Beziehung.[31] Ähnlich wird auch das Phänomen des „Cyberflashing"[32] – eine Form des Online-Exhibitionismus,[33] also das unaufgeforderte Zusenden intimer Fotos oder Videos (umgangssprachlich als „Nudes" oder „Dick Pics" bezeichnet) an eine Person, die nicht in den Erhalt solcher Dateien eingewilligt hat – teilweise als IBSA verstanden. Darüber hinaus umfasst IBSA auch die Erstellung und/oder Verbreitung manipulierter sexueller Darstellungen, etwa in Form von „Deep Fakes", KI-generierten pornografischen Bildern[34] oder „sexualisiertem Photoshopping".

Teilweise wird auch die „bildbasierte sexuelle Erpressung" als besondere Erscheinungsform von IBSA begriffen. Sie tritt etwa als Nötigung einer Person, intime oder sexuelle Fotos oder Videos von sich selbst zu erstellen und/oder zu teilen, als Nötigung einer Person durch die Androhung der Verbreitung solcher Daten oder in Formen des Abfangens bzw. Beschaffens intimer Aufnahmen, z.B. durch Hacken einer Webcam oder eines Datenspeichers, auf.

Die Vielzahl der unter IBSA subsumierten Verhaltensweisen richtet sich gegen mehrere Schutzgüter (zugleich) – namentlich die sexuelle Selbstbestimmung,[35] die informationelle Selbstbestimmung,[36] das Recht am eigenen Bild,[37] die persönliche Ehre[38] – und verdeutlicht die Notwendigkeit einer begrifflichen Abgrenzung, um eine tragfähige konzeptionelle Definition zu entwickeln. Dabei können mehre-

31 *McGlynn/Rackley/Houghton*, Continuum of IBSA (Fn. 10), S. 29; *Fido/Harper*, Image-Based Sexual Offending (Fn. 9), S. 4.

32 *Hall/Hearn/Lewis*, IBSA (Fn. 1), S. 327; *Fido/Harper*, Image-Based Sexual Offending (Fn. 9), S. 9 f.; *Andresen/Dreyer*, Online-Formen aufgezwungener Sexualität (Fn. 19), S. 2.

33 *Fido/Harper*, Image-Based Sexual Offending (Fn. 9), S. 10.

34 Vgl. zu pornografischen Deepfakes *T. Crone*, Bildbasiert aber unsichtbar: Warum pornografische Deepfakes eigenständig verboten werden müssen, VerfBlog vom 23.1.2026, abrufbar unter: <https://verfassungsblog.de/pornografische-deepfakes/>, zuletzt abgerufen am 18.2.2026.

35 So auch *S. Beck/M. Nussbaum*, KI ohne Verantwortung? Grok, X und sexualisierte Deepfakes, VerfBlog 16.2.2026, abrufbar unter <https://verfassungsblog.de/ki-grok-deepfakes-strafrecht/>, zuletzt abgerufen am 18.2.2026; *Sanow*, Voyeuristische Bildaufnahmen (Fn. 3), S. 69 ff.

36 Nach *Schmidt*, Pornographie (Fn. 16), S. 247: das Recht auf sexuelle Selbstbestimmung *i.V.m.* dem Recht auf informationelle Selbstbestimmung.

37 So auch *N. Dinig*, Zivilrechtliche Interventionen bei digitaler Gewalt, in: bff/Prasad (Hrsg.), Geschlechtsspezifische Gewalt (Fn. 2), S. 151 (164 f.); *Sanow*, Voyeuristische Bildaufnahmen (Fn. 3), S. 68 f.

38 *C. Clemm*, Möglichkeiten und Grenzen strafrechtlicher Interventionen bei digitaler Gewalt, in: bff/Prasad (Hrsg.), Geschlechtsspezifische Gewalt (Fn. 2), S. 129 (130 f.); krit. jdf. zu einer Reduktion auf die Ehrdelikte *Schmidt*, Pornographie (Fn. 16), S. 212 bzw. S. 338, vgl. auch S. 357, jew. m.w.N.; *Sanow*, Voyeuristische Bildaufnahmen (Fn. 3), S. 162.

re Handlungsformen (Erstellung/Manipulation, Versand/Verbreitung, Beschaffung und Nötigung) – je nach Kontext, betroffener Person und Inhalt der Aufnahmen bzw. Daten – eine Handlung zu IBSA, präziser und die Datafizierung direkt berücksichtigend: zu DBSA, machen.

<table>
<tr><th>Verwendetes Material →
Handlung ↓</th><th colspan="2">Einvernehmlich erstellte Bilder</th><th>Nicht einvernehmlich erstellte Bilder</th><th>Nicht einvernehmlich mit KI erstellte oder veränderte Bilder</th></tr>
<tr><td>Erstellung/Veränderung</td><td colspan="2">—</td><td>Nicht einvernehmliche Pornografie
Nicht einvernehmliche intime Bilder (z. B. Upskirting / Downblousing)
Aufnahmen mit versteckten Aufnahmegeräten</td><td>Sexualisierte Bildbearbeitung
Deepfakes
KI-generierte pornografische Bilder</td></tr>
<tr><td rowspan="2">Nicht einvernehmliches Versenden/Verbreiten</td><td>an andere</td><td colspan="3">Rachepornos</td></tr>
<tr><td>an das Opfer</td><td colspan="3">Cyberflashing (unaufgefordertes Versenden von intimen/sexuellen Bilder, z. B. sog. „Dick Pics”)
Bei Verwendung als Mittel zur Nötigung: möglicherweise bildbasierte sexuelle Erpressung</td></tr>
<tr><td>Nicht einvernehmliche Beschaffung/Erlangung</td><td colspan="2">Phishing</td><td colspan="2">Kauf/Streaming von nicht einvernehmlich erstellten intimen Bildern</td></tr>
<tr><td>Nötigung</td><td colspan="4">Bildbasierte sexuelle Erpressung/Nötigung</td></tr>
</table>

Die Aufstellung verdeutlicht, dass das Problem aus einer anderen Perspektive beschrieben werden muss, um die tatsächlichen Schutzlücken zu adressieren. Hierfür bedarf es gemeinsamer Faktoren der aufgezeigten Phänotypen (B.I.), woraus sich eine Clusterbildung der Datentypen sowie eine Einteilung in Handlungsebenen (B.II.) und deren Dimensionen (B.III.) ergibt.

I. Parallelen der aufgezeigten Phänotypen

Die Unterscheidung zwischen spezifischen Datentypen sowie eine Differenzierung nach Täter:innen, Betroffenen oder der Quantifizierung einzelner Erscheinungsformen hat sich als wenig zielführend erwiesen. Um zu einer tragfähigen Definition zu gelangen, die sowohl die oben beschriebenen Phänomene als auch typische Datenphänomene umfasst, müssen die zahlreichen und unscharfen Phänotypen strukturiert werden. Insgesamt lassen sie sich in zwei Hauptcluster einteilen.

Cluster 1 umfasst alle Arten sexueller Gewalt, die mittels **authentischer Daten** begangen werden. Erfasst sind alle Datentypen, die auf tatsächlich stattgefundenen Handlungen beruhen bzw. diese darstellen, etwa eine unveränderte Foto- oder Videoaufnahme.

Cluster 2 umfasst sexuelle Gewalt unter Verwendung nicht-authentischer oder **verfälschter Daten**. Dazu gehören vollständig erfundene Inhalte wie textliche Beschreibungen frei erfundener Ereignisse (unabhängig davon, ob sie von einem Menschen oder einer NLP-KI erstellt wurden) oder vollständig KI-generierte Bilder.

Eine Herausforderung stellt die Unterscheidung zwischen authentischen und nicht authentischen Daten in Grauzonen dar: Es stellt sich etwa die Frage, ob Änderungen an ursprünglich authentischen Daten durch KI, Photoshop oder andere Manipulationssoftware noch als authentische Daten eingestuft werden können und wo die Grenzen liegen. So lässt sich vortragen, dass es dafür hinreiche, wenn trotz Bearbeitung die Bedeutung, der semantische Gehalt und der Kontext des ursprünglichen Materials noch erkennbar bleiben.[39] Eine Grenzziehung wäre aber auch dahingehend denkbar, dass der wesentliche Informationswert der Daten weiter bestimmend sein müsse. Dann würden Daten, die zwar aus authentischen Daten stammen, aber so verändert oder manipuliert wurden, dass Bedeutung, Inhalt oder Kontext in den resultierenden Daten nicht mehr bestimmend hervorgehen, dem zweiten Cluster zufallen.

Bei genauer Betrachtung jener erforderlichen Differenzierung zwischen gefälschten und authentischen Daten zeigen sich erkennbar Parallelen zu den Vorschriften zur Urkundenfälschung im deutschen Strafrecht. § 267 Abs. 1 StGB umfasst drei Handlungsformen: das Herstellen einer unechten Urkunde, das Verfälschen einer echten Urkunde und das Gebrauchen einer unechten oder verfälschten Urkunde. Eine Urkunde i.S.d. Norm ist eine verkörperte menschliche Gedankenerklärung (*Perpetuierungsfunktion*), die als Beweismittel im Rechtsverkehr geeignet und bestimmt ist (*Beweisfunktion*) und die ihren Aussteller erkennen lässt (*Garantiefunktion*).[40] Alle drei Begehungsvarianten setzen die Absicht voraus, zum Zwecke der Täuschung im Rechtsverkehr zu handeln. Die Täuschungshandlung muss darauf gerichtet sein, den Adressaten zu einem rechtserheblichen Verhalten zu veranlas-

39 Ähnl. etwa die Erwägung Nr. 19 der RL (EU) 2024/1385, die wohl (auch) auf den objektiven Empfängerhorizont abstellt: Hiernach sollen auch „Deepfakes" erfasst sein, „bei denen das Material einer existierenden Person, […] oder anderen Einheiten oder Ereignissen, die sexuelle Handlungen einer Person darstellen, deutlich ähnelt und anderen Personen fälschlicherweise als authentisch oder wahrheitsgemäß erscheinen würde".

40 *M. Weidemann*, in: B. von Heintschel-Heinegg (Hrsg.), Beck'scher Online-Kommentar StGB, 67. Aufl., München 2025, § 267 Rn. 33 ff.

sen.[41] Nach h.M. schützt der Straftatbestand die Sicherheit und Zuverlässigkeit des Rechtsverkehrs, insbesondere den Beweisverkehr mit Urkunden.[42]

Handlungen aus Cluster 2 lassen sich freilich nicht unmittelbar unter den Tatbestand der Urkundenfälschung subsumieren; das ist hier auch nicht gemeint. Die hier relevanten Daten werden kaum jemals verwendet, um rechtsverbindliche Handlungen herbeizuführen. Zudem erfüllen digitale Daten regelmäßig nicht die Urkundendefinition: Zwar mag die Garantiefunktion in Fällen, in denen die abgebildete Person erkennbar ist, als erfüllt angesehen werden. Gleichwohl bleibt es schwierig, speicherbare Daten als „verkörpert" zu qualifizieren.[43] Diese Einschränkungen sind hier jedoch nicht maßgebend. Der angestellte Vergleich dient vielmehr als dogmatische Grundlage, um einen strafrechtlichen Zugang für die in Cluster 2 beschriebenen Handlungen zu entwickeln. Das ist im Wesentlichen aus zwei Gründen sachgerecht:

(1) Die in § 267 Abs. 1 StGB beschriebenen Tathandlungen ähneln den in Cluster 2 dargestellten Verhaltensweisen. Darin liegt ein erster und wichtiger Ansatz, um diese Formen missbräuchlichen Verhaltens strafrechtlich zu erfassen: aktuell existiert keine Legaldefinition und kein arbeitsfähiger juristischer Begriff für DBSA (oder IBSA). Das Anknüpfen an etablierte Begriffe kann hilfreich sein, um neue Rechtsbegriffe und legislative Maßnahmen einzuführen.

(2) Das geschützte Rechtsgut der Urkundenfälschung – die Sicherheit und Zuverlässigkeit des Rechtsverkehrs[44] – weist eine inhaltliche Parallele zum Problem „gefälschter" Daten (Cluster 2) auf.[45] Einer Ansicht zufolge schützt die Norm auch Einzelne, deren Beweisposition (d.h. Glaubwürdigkeit) durch die Verfälschung einer Urkunde beeinträchtigt wird (etwa durch den Missbrauch eines Namens oder die Aushändigung untauglicher Beweismittel).[46] Dieser Schutzgedanke lässt sich auf jene Personen übertragen, die in manipulierten Daten (unzutreffend) dargestellt werden. Gerade die den DBSA-Phänomenen z.T. innewohnende Verbindung zwischen der Verletzung der sexuellen *und* der informationellen Selbstbestimmung[47]

41 *V. Erb*, in: V. Erb/J. Schäfer (Hrsg.), Münchener Kommentar zum StGB, Bd. 5, 5. Aufl., München 2025, § 267 Rn. 205.

42 *Weidemann* (Fn. 40), § 267 Rn. 2.

43 Vgl. auch *Blocher*, Strafbare Deepfakes (Fn. 10), S. 228.

44 *I. Puppe/K. Schumann*, in: U. Kindhäuser/U. Neumann/H. Paeffgen/F. Saliger (Hrsg.), NomosKommentar Strafgesetzbuch, 6. Aufl., Baden-Baden 2023, § 267 Rn. 1.

45 Vertiefend zur Vergleichbarkeit der Schutzbedürfnisse *Blocher*, Strafbare Deepfakes (Fn. 10), S. 228 f.

46 *G. Heine/F. Schuster*, in: J. Eisele (Hrsg.), Tübinger Kommentar Strafgesetzbuch, 31. Aufl., München 2025, § 267 Rn. 1 m.w.N.

47 Zur systematischen Verortung und zur primären Betroffenheit der sexuellen Selbstbestimmung vgl. auch *B. Burghardt*, Zur kriminalisierungstheoretischen Berücksichtigung von strukturellen Machtasymmetrien und Ungleichheiten, in: Burghardt et al. (Hrsg.), Sexuelle Selbstbestimmung (Fn. 27), S. 131 (140).

kann über einen solchen Tatbestand erfasst werden; denkbar ist etwa der Aufbau als Grunddelikt (Falschdarstellung) und Qualifikation oder Regelbeispiel (sexualisierte Falschdarstellung).

Die zunehmende Datafizierung menschlicher Kommunikation betrifft mittlerweile sämtliche gesellschaftlichen Bereiche[48] – und sämtliche Daten werden zunehmend kommerzialisiert bzw. monetarisiert.[49] Diese Entwicklung birgt erhebliche Gefahren nicht nur für Kommunikationssysteme und -räume, sondern auch für politische und damit rechtliche Systeme.[50] Datenhandel schafft nicht nur eine weitere Dimension der Kommunikation, sondern eröffnet zugleich neue Missbrauchspotentiale. Sexuelle Kommunikation ist dabei ein besonders sensibler Bereich der menschlichen Interaktion, da sie sowohl die intimsten Bereiche des Menschen als auch hochrangige Rechtsgüter betrifft. Der Schutz der informationellen Privatsphäre als Aspekt und Ausdruck persönlicher Autonomie[51] durch das Strafrecht ist daher insbesondere dann notwendig, wenn ein sexualisierter Datenmissbrauch droht.[52]

II. Einteilung in Handlungsebenen

Unterteilt man, dem folgend, die identifizierten Faktoren, geordnet nach den beiden Clustern, in Handlungsebenen, ergibt sich ein konzeptioneller (Neu)Ansatz: Handlungen nach **Cluster 1** (authentische Daten), setzen eine vorgelagerte natürliche (einvernehmliche oder nicht einvernehmliche) Handlung voraus, die in irgendeiner Form datenvermittelt dargestellt oder abgebildet wird. In dieser natürlichen Handlung kann, muss aber nicht zwingend, bereits eine Rechtsgutsverletzung liegen. Auf der zweiten Ebene der (möglichen) Rechtsgutsverletzung werden Daten mit oder ohne Zustimmung **erstellt**. Auf Ebene 3 können diese Daten wiederum mit oder ohne Zustimmung **verbreitet** werden.

48 Vgl. auch *L. Wörner*, Code is creates law, POLITIKUM 2023, S. 64.

49 Zur Monetarisierung von Beziehungen in sozialen Medien und der sich entwickelnden Transaktionskultur vgl. *J. Ringrose/K. Regehr/B. Milne*, Understanding and Combatting Youth Experiences of Image-Based Sexual Harassment and Abuse (Association of School and College Leaders), S. 12, online abrufbar unter <https://www.ascl.org.uk/ASCL/media/ASCL/Our%20view/Campaigns/Understanding-and-combatting-youth-experiences-of-image-based-sexual-harassment-and-abuse-full-report.pdf>, zuletzt abgerufen am 15.1.2026 m.w.N.

50 Vgl. z.B. *J. Redden*, Democratic governance in an age of datafication: Lessons from mapping government discourses and practices, 5 Big Data & Society 2018, eLocator: 2053951718809145.

51 *B. Rössler*, Privatheit, Autonomie, Recht, in: S. Baer/U. Sacksofsky (Hrsg.), Autonomie im Recht – Geschlechtertheoretisch vermessen, Baden-Baden 2018, S. 97 (99).

52 Vgl. z.B. EGMR 56867/15 (2020, *Buturugă v. Rumänien*), Nr. 40, 74 mit Spezifizierung von IKT- (Informations- und Kommunikationstechnologie) bezogenen Verletzungen der Privatsphäre und Cybergewalt; siehe auch EGMR 40419/19 (2021, *Volodina gegen Russland (Nr. 2)*), Nr. 23f., 67f., in dem die positive Verpflichtung des Staates zum Schutz des Rechts auf Achtung des Privatlebens (Art. 8 EMRK) vor Cybergewalt (einschließlich der Veröffentlichung intimer Fotos) als verletzt angesehen wird. Vgl. weiterführend und m.w.N. auch *Schmidt*, Pornographie (Fn. 16), S. 171 sowie *dies.*, Expertise zur Kriminalisierung sexualisierender Deepfakes, unveröffentlichtes Gutachten für HateAid, S. 28 ff., die für die Schaffung eines speziellen Straftatbestands plädiert.

Zur Veranschaulichung werden die Ebenen anhand der folgenden **Beispiele** erläutert:

	Abgebildete Person(en) hat/haben zugestimmt	**Abgebildete Person(en) hat/haben nicht zugestimmt**
Dargestellte (natürliche) Handlung	– einvernehmliche sexuelle Handlungen zwischen zwei oder mehr Erwachsenen – sexuelle Handlungen allein der abgebildeten Person – Verhalten, das nicht sexuell ist, aber in einer intimen Umgebung stattfindet und sexualisiert werden könnte (z.B. Duschen, Entkleiden usw.)	– Vergewaltigung
Erstellung der Daten	– einvernehmliche Aufzeichnung einvernehmlicher sexueller Handlungen – Selbstaufzeichnung sexueller Handlungen	– Aufzeichnung erfolgte ohne oder gegen den Willen des Opfers – ein Foto oder Video des Opfers wurde erheblich verändert, um etwas anderes darzustellen als die ursprüngliche Bedeutung des Bildes (z.B. Verwendung von Deepfake-Technologie, um ein pornographisches Video mit dem Gesicht und/oder Körper einer Person zu erstellen)
Verbreitung der Daten	– die abgebildete Person lädt die Bilder selbst hoch (z. B. auf Plattformen wie OnlyFans) – die abgebildete Person hat der Veröffentlichung zugestimmt	– Versenden (einvernehmlich erstellter) intimer Fotos des Opfers an andere ohne dessen Zustimmung („Revenge Porn“)

Die Phänotypen, die unter **Cluster 2** (gefälschte Daten) fallen, sind definitionsgemäß nicht das Ergebnis einer natürlichen Handlung, jedenfalls nicht in der Weise, wie sie durch die Daten dargestellt wird. Ebene 1 wird hier daher irrelevant. Auf Ebene 2, der Erstellung der Daten, stellt sich die Frage, ob und wer für welche Handlungen strafrechtlich verantwortlich gemacht werden kann. Die Grenzen der Kunst- und Meinungsfreiheit sind zu wahren, Strafrecht darf nur zurückhaltend eingesetzt werden.[53] Enthält pornografisches Material keine konkrete, reale Per-

53 *L. Wörner*, Straf(*rechts*)würdigkeit, -bedürftigkeit, -tauglichkeit und Schutzfähigkeit – zur Ordnung eines »phänomenalen« Argumentationsstraußes –, in: M. Kuhli/M. Asholt (Hrsg.), Strafbegründung und Strafeinschränkung als Argumentationsmuster, Baden-Baden 2017, S. 97 (110 f.); speziell zur Kriminalisierung im Netz vgl. *L. Wörner/N. Preetz*, The New German Darknet-Criminal Law-Draft – Darkening by Restricting Individual Rights – Ceza Hukuku ve Kriminoloji Dergisi-Journal of Penal Law and Criminology 2020, S. 33 (48 f.), jew. m.w.N. Zu den Risiken der Einschränkung von Meinungsfreiheit im digitalen Raum vgl. auch *J. Moolman/H. Kamran/E. Smith*, Freedom of Expression and Participation in Digital Spaces, in: UN Women Expert Group Meeting 2022, online

son, kommt eine strafrechtliche Verantwortlichkeit nur in Betracht, wenn besonders schutzbedürftige Personengruppen (Kinder/Jugendliche, vgl. § 184b f. StGB) dargestellt werden, Inhalte besonders schutzbedürftigen Personengruppen (Kinder/Jugendliche, vgl. § 184 StGB) zugänglich gemacht oder wenn besonders „anstößige" bzw. sittenwidrige Inhalte (Gewalt- oder Tierpornografie, vgl. § 184a StGB) gezeigt werden.

III. Dimensionen, Ebenen und Geschlechtsspezifität

Die Vielschichtigkeit von DBSA spiegelt sich daher nicht nur in der Vielfalt ihrer Erscheinungsformen wider. Unabhängig vom konkreten Typ sind die Handlungsebenen einer höheren Eingriffsintensität zugänglich, als sie von anderen Straftaten bekannt ist:

1. Niedrigschwelligkeit der Täterwerdung

Die leichte Zugänglichkeit der Tatmittel sowie die Trivialisierung und Allgegenwärtigkeit datenbasierter sexueller Übergriffe vereinfachen und verharmlosen den Prozess der Täterwerdung. Nicht nur Pornografie-Websites profitieren finanziell von der sexuellen Verrohung ihrer Nutzer. Die durch bestimmte Onlineplattformen gewährte Anonymität und die durch ihre Algorithmen erzeugte Anreizstruktur laden geradezu zur Erstellung und zum Hochladen sexuell missbräuchlicher Inhalte ein oder tolerieren diese zumindest; viele Anbieter profitieren von dem durch sexuelle Inhalte erzeugten „Traffic". Der Zugang zu datenbasierten Sexualdelikten ist für potenzielle Täter mithin äußerst niedrigschwellig.

2. Viktimisierung, Sphären und Intensität der Rechtsgutsverletzung

Auf der anderen Seite führen die zunehmende Nutzung aller Arten von Social-Media-Plattformen, die zunehmend umfassende Datafizierung von Kommunikation und die abgestumpfte soziale Wahrnehmung missbräuchlicher Verhaltensweisen dazu, dass Nutzer:innen immer anfälliger für eine DBSA-bezogene Viktimisierung werden. Das Viktimisierungsrisiko ist insgesamt hoch, insbesondere aber ungleich verteilt, was Faktoren wie Geschlecht, Alter, Sexualität und ethnische Zugehörigkeit betrifft.[54] Die Grenze zwischen Täter- und Opferrolle verschwimmt.[55] DBSA kann einerseits die intimsten Lebensbereiche der Betroffenen mindestens ebenso

abrufbar unter: <https://www.unwomen.org/sites/default/files/2022-12/EP.14_Jan%20Moolman.pdf>, zuletzt abgerufen am 10.1.2026, S. 17 ff.

54 *E. Rackley/C. McGlynn/K. Johnson/N. Henry/N. Gavey/A. Flynn/A. Powell*, Seeking Justice and Redress for Victim-Survivors of Image-Based Sexual Abuse, 9 Feminist Legal Studies 2021, S. 293 (299).

55 Vgl. z.B. *B. Sparks/S. Stephens/S. Trendell*, Image-Based Sexual Abuse: Victim-Perpetrator Overlap and Risk-Related Correlates of Coerced Sexting, Non-Consensual Dissemination of Intimate Images, and Cyberflashing, Computers in Human Behavior 2023, 107879 (7) m.w.N.

stark beeinträchtigen wie die etablierteren Sexualstraftaten.[56] In schwereren Fällen wird die Sexualität des Opfers der Öffentlichkeit irreversibel preisgegeben. Jeder kann die dargestellten Vorfälle sehen, was es Betroffenen nahezu unmöglich macht, eine ohnehin schon traumatische Erfahrung zu verarbeiten. Andererseits haben sich bestimmte Praktiken, die als IBSA bzw. DBSA klassifiziert werden, zu einem fast alltäglichen Phänomen[57] entwickelt. Das unerwünschte Empfangen intimer Fotos (z.B. sog. „Dick Pics") gilt so heute als bekanntes Risiko, wenn nicht gar als bagatellisierter Bestandteil der Nutzung von Online-Dating-Plattformen. Dass DBSA im Alltag beinahe selbstverständlich erscheinen, ändert nichts daran, dass sie für individuelle Betroffene schwerwiegende Schäden verursachen. Die Stigmatisierung der eigenen Sexualität und die Scham rund um sexuellen Missbrauch sind nach wie vor allgegenwärtig; Praktiken der Opferbeschuldigung („Warum hat sie die Fotos überhaupt gemacht, wenn sie nicht wollte, dass sie veröffentlicht werden?") sind weiterhin ein beliebtes Mittel, um die Verantwortung von den Täter:innen auf die Opfer abzuwälzen.[58] Viele dieser soziokulturellen Muster können Opfer einem hohen Risiko einer sekundären Viktimisierung aussetzen, nicht selten auch durch Strafverfolgungsbehörden.[59]

Zuletzt wurden die problematischen Folgen mittels erheblicher Bemühungen in Forschung, Zivilgesellschaft[60] und Politik[61] sichtbarer gemacht; sie erfuhren und erfahren politische Aufmerksamkeit. Teils haben sie zu gesetzgeberischen Maßnahmen geführt.[62] Gleichwohl wird sexuelle Gewalt häufig nicht als solche erkannt; selbst strukturell gleichförmig auftretende Phänomene werden individualisiert. Behörden stehen bei der Verfolgung digitaler Straftaten regelmäßig vor erheblichen Herausforderungen: die Identifizierung der Täter:innen,[63] Beweisführung, Fragen der Gerichtsbarkeit bzw. Zuständigkeit usw. Die Kombination sexueller und digi-

56 In Bezug auf die Folgen für Opfer von DBSA wird teilweise der Begriff „virtuelle Vergewaltigung" verwendet, vgl. etwa *K. Jarvers*, Der „Codice Rosso": Neue Maßnahmen gegen geschlechtsbezogene und häusliche Gewalt in Italien, ZStW 2022, S. 805, (825 f.) m.w.N.; *Rackley/McGlynn/Johnson/Henry/Gavey/Flynn/Powell*, Seeking Justice (Fn. 54), S. 303.

57 Vgl. etwa *J.-K. Bauer/A. Hartmann/N. Prasad*, Einleitung, in: bff/Prasad (Hrsg.), Geschlechtsspezifische Gewalt (Fn. 2), S. 9 (12).

58 Vgl. auch *Beck/Nussbaum*, KI ohne Verantwortung (Fn. 35).

59 *R. Campbell*, The Psychological Impact of Rape Victims' Experiences with the Legal, Medical, and Mental Health Systems, The American psychologist 2008, S. 702 (703 f.).

60 Vgl. etwa djb e.V., Policy Paper st23–17: Bekämpfung bildbasierter sexualisierter Gewalt; Hanna Seidel und Ida Marie Sassenberg, „Petition „#Upskirting in Deutschland unter Strafe stellen!" ('Verbietet Upskirting in Deutschland!')" (*change.org,* 3.4.2019), online abrufbar unter <https://www.change.org/p/verbietet-upskirting-in-deutschland>, zuletzt abgerufen am 7.1.2026.

61 Vgl. nur beispielhaft die Antworten der Bundesregierung auf Kleine Anfragen: „Digitale Gewalt gegen Frauen", BT-Drs. 19/6174 (2018); „Datenlage zu verschiedenen Formen digitaler Gewalt, Regelungslücken und Handlungsbedarf", BT-Drs. 20/9543 (2023).

62 Vgl. die in Fn. 60 genannte Petition; 2020 wurde mit dem 59. StÄndG zur Verbesserung des Persönlichkeitsschutzes bei Bildaufnahmen vom 9.10.2020 (BGBl. I 2020, 2075) dann § 184k StGB eingefügt.

63 *Clemm*, Digitale Gewalt (Fn. 38), S. 140 ff.

taler Delikte, die geschlechtsspezifische Viktimisierung sowie die Schwierigkeiten in der Definition, Bekämpfung und Regulierung von DBSA führen zu einer gewissen Zurückhaltung – wenn nicht sogar zu einem Unwillen[64] – bei der Strafverfolgung. Tatsächlich ist die Strafverfolgung im digitalen Raum ein nahezu unmögliches Unterfangen. Diese Faktoren können den (potenziellen) Schaden, der durch DBSA verursacht wird, erheblich verstärken. Dabei könnte die Datafizierung von Sexualität zugleich die Beweisbarkeit von sexueller Gewalt erheblich erleichtern, indem sie diese sichtbar – datafiziert – macht. Doch die datenbasierte Dokumentation wirkt sich in der Realität bislang nahezu ausschließlich negativ auf die Betroffenen aus, indem sich die schädlichen Auswirkungen primärer Viktimisierung intensivieren und das Risiko sekundärer Viktimisierung erhöht wird.

3. Geschlechtsspezifität

Sexuelle Gewalt weist insgesamt und global eine deutliche Geschlechtsspezifität auf: Die meisten Opfer sind weiblich, die meisten Tatverdächtigen männlich.[65] Bei diesen Statistiken müssen allerdings verzerrende Faktoren berücksichtigt werden, insbesondere die hohe Dunkelziffer bei Sexualdelikten: Opfer zögern häufig, sexuelle Gewalt zur Anzeige zu bringen, oder werden aufgrund sozialer Stigmatisierung, Scham und Angst vor der Konfrontation mit dem Täter und vor den Folgen nicht ernst genommen[66].[67] Trotz der Allgegenwärtigkeit von DBSA-Vorfällen und der oft öffentlichen Dokumentation der Taten ist die Datenlage für die statistische Auswertung unzureichend.[68] Selbst unter Berücksichtigung all dieser Faktoren lässt

64 Vgl. *B. Valerius*, Das geplante „Gesetz gegen Digitale Gewalt, ZRP 2023, S. 142 (143 f.), der die Verlagerung der Strafverfolgung auf die betroffene Person/das Opfer in Fällen von Cybergewalt kritisch analysiert.

65 Für Deutschland siehe die jährlichen PKS-Tabellen des BKA 3 „04_Vergewaltigung, Sexuelle Nötigung und Sexuelle Übergriffe", online abrufbar unter <https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/pks_node.html>, zuletzt abgerufen am 7.1.2026; für die USA vgl. z.B. *RAINN (Rape, Abuse & Incest National Network)*, Victims of Sexual Violence: Statistics, online abrufbar unter <https://www.rainn.org/statistics/victims-sexual-violence>; für einen detaillierten Überblick siehe *UNODC*, Victims of Sexual Violence, online abrufbar unter <https://dataunodc.un.org/dp-crime-victims-sexual-violence>, beide zuletzt abgerufen am 15.1.2026.

66 *Campbell*, Psychological Impact (Fn. 59), S. 7034 f.; vgl. auch *M. Bagherian/Z. Hashemi Dezaki/B. Bahmani*, The Big Role of Authority, Sanctity, and Modern Myths about Sexual Aggression in Blaming the Rape Victims: A Study on Culture of Honor, PsyArXiv 2021 2, online abrufbar unter <https://osf.io/jz6xe>, zuletzt abgerufen am 15.1.2026, S. 1 f. m.w.N.

67 Vgl. z.B. *Bagherian/Dezaki/Bahmani*, Culture of Honor (Fn. 66), S. 12 f. m.w.N.

68 *EIGE (European Institute for Gender Equality)*, Combating Cyber Violence Against Women and Girls2022, online abrufbar unter 8 <https://eige.europa.eu/sites/default/files/documents/combating_cyber_violence_against_women_and_girls.pdf>, zuletzt abgerufen am 10.1.2026, S. 38 in Bezug auf die statistische Erfassung aller Formen von Cybergewalt.

sich jedoch eine geschlechtsspezifische Dimension digitaler sexualisierter Gewalt[69] ebenso festhalten wie die Tatsache, dass Frauen insgesamt einem höheren Risiko sexueller Objektivierung[70] und sexueller Gewalt ausgesetzt sind als Männer.[71] Im spezifischen Kontext von DBSA kommen Studien jedoch zu unterschiedlichen Ergebnissen. Mehrere Untersuchungen zu Cybergewalt auf EU-, internationaler und nationaler Ebene zeigen, dass Frauen und Mädchen in hohem Maße davon betroffen sind.[72] Andere Studien weisen vergleichbare Viktimisierungsraten für Frauen und Männer aus.[73] Ungeachtet dessen variieren die Erfahrungen mit den Auswirkungen und der Täterschaft je nach Geschlecht, Alter und Sexualität.[74] Weibliche Internetnutzerinnen werden insgesamt häufiger Opfer schwerer Formen von Cybergewalt.[75]

IV. Konzeptualisierung und Begriffsbestimmung

Unter Berücksichtigung der vorangegangenen Überlegungen lässt sich der Begriff „datenbasierte sexuelle Gewalt" mit folgenden wesentlichen Elementen konzeptualisieren:[76]

1. Die Nicht-Einvernehmlichkeit einer oder mehrerer Ebenen der Handlung

Wie bereits gezeigt, gibt es im Zusammenhang mit DBSA mehrere Ebenen möglicher Rechtsverletzungen, die jeweils die Gesamtintensität steigern. Liegt bezüglich

69 Vgl. etwa *N. Prasad*, Digitalisierung geschlechtsspezifischer Gewalt – Zum aktuellen Forschungsstand, in: bff/Prasad (Hrsg.), Geschlechtsspezifische Gewalt (Fn. 2), S. 17 (17 ff.); *U. Lembke*, Menschenrechtlicher Schutzrahmen für Betroffene von digitaler Gewalt, in: bff/Prasad (Hrsg.), Geschlechtsspezifische Gewalt (Fn. 2), S. 47 (49 ff.) m.w.N.; *Sanow*, Voyeuristische Bildaufnahmen (Fn. 3), S. 54 f. m.w.N.

70 *M. Dvir/M. Nagar*, Would Victims Blame Victims? Effects of Ostracism, Sexual Objectification, and Empathy on Victim Blaming, 3 Frontiers in psychology 2022, 912698 (1).

71 *Schmidt*, Pornographie (Fn. 16), S. 353 f. zur besonderen Vulnerabilität von Frauen und Mädchen gegenüber sexueller Belästigung.

72 Laut der *EIGE*-Studie (Fn. 68), S. 37 sind Frauen und Mädchen häufiger Ziel von Cybergewalt und im Allgemeinen als Opfer überrepräsentiert.

73 *A. Powell/A. Scott/A. Flynn/S. McCook*, A Multi-Country Study of Image-Based Sexual Abuse: Extent, Relational Nature and Correlates of Victimisation Experiences, The Journal of Sexual Aggression 2022, S. 1 (8); siehe auch *Rackley/McGlynn/Johnson/Henry/Gavey/Flynn/Powell*, Seeking Justice (Fn. 54), S. 299 m.w.N.

74 *Rackley/McGlynn/Johnson/Henry/Gavey/Flynn/Powell*, Seeking Justice (Fn. 54), S. 299; *F. Staude-Müller/B. Hansen/M. Voss*, How Stressful Is Online Victimization? Effects of Victim's Personality and Properties of the Incident, The European Journal of Developmental Psychology 2012, S. 260; *Pew Research Center*, The State of Online Harassment, online abrufbar unter <https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2021/01/PI_2021.01.13_Online-Harassment_FINAL-1.pdf>, zuletzt abgerufen am 15.1.2026; *EIGE*-Studie (Fn. 68), S. 378 f. m.w.N.; vgl. auch djb e.V., Policy Paper: Zugang zu Recht in Fällen digitaler Gewalt, Manuskript-S. 3 (im Erscheinen).

75 *R. Almenar*, Cyber Violence against Women and Girls: Gender-based Violence in the Digital Age and Future Challenges as a Consequence of Covid-19, Trento Student Law Review 2021, S. 167 (170) m.w.N.

76 Zielsetzung ist dabei nicht die Entwicklung eines Tatbestands de lege ferenda, sondern vielmehr die Schaffung einer Arbeitsdefinition als Forschungsbegriff für bestimmte Fallgruppen.

aller Handlungsebenen eine freie und umfassende Einwilligung[77] der betroffenen Person vor, sind keine relevanten Rechtsgüter verletzt, sodass kein Bedarf an Kriminalisierung besteht. Das Einverständnis zu einer bestimmten Ebene setzt jedoch stets das Einverständnis zu der/den vorherigen Ebene(n) voraus. Fehlt das Einverständnis auf einer der Ebenen, so setzt sich dieser Mangel auf den nachfolgenden Ebenen fort, sodass ein Fall der datenbasierten sexuellen Gewalt bereits dann vorliegt, wenn eine natürliche Handlung entweder nicht-einvernehmlich datafiziert wird oder einvernehmlich erzeugte Daten ohne Einverständnis verbreitet werden. In Fällen, in denen sowohl die Erstellung von Daten als auch deren Verbreitung ohne Zustimmung erfolgen, wird die Rechtsverletzung weiter verstärkt.[78] Das Fehlen des Einverständnisses auf der zweiten Ebene (Herstellung der Daten) reicht folglich aus, um datenbasierte sexuelle Gewalt anzunehmen; das Vorhandensein der dritten Ebene (Verbreitung) ist insoweit fakultativ:

77 Dabei reicht das bloße Fehlen eines Widerspruchs nicht aus; zu einer ausführlichen Diskussion über den Unterschied zwischen „Ja heißt Ja" und „Nein heißt Nein" im Kontext des deutschen Strafrechts vgl. *L. Gmelin/H. Wörner*, Reform Needs in German Criminal Law on Sexual Offenses. The Non-Compromise of „No-Means-No", in: R. Erbaş (Hrsg.), European Perspectives on Attrition in Sexual Offenses, Lexington Books, Lanham 2023. Zur Frage der wirksam erteilten Einwilligung ebd. S. 87 ff., 92 ff.

78 Die durch die ursprüngliche Sexualstraftat verursachte Rechtsgutsverletzung wird erheblich intensiviert – zum einen, weil die nicht einvernehmliche Datenerfassung selbst eine Rechtsgutsverletzung darstellt; zum anderen, weil die Datenerfassung eine Verkörperung und dauerhafte Abrufbarkeit in der Öffentlichkeit bewirkt, was psychologische Heilungsprozesse erheblich beeinträchtigen kann. Darüber hinaus besteht die Gefahr einer sekundären Viktimisierung durch die Verwendung solcher Daten als Mittel der Nötigung, vgl. etwa *McGlynn/Rackley/Houghton*, Continuum of IBSA (Fn. 10), S. 35.

Ebene	Einverständnis des Opfers / der abgebildeten Person			
Dargestellter sexueller Akt	(-)	(+)	(+)	(+)
Erstellung der Daten	(-)	(-)	(+)	(+)
Verbreitung der Daten	*(-) fakultativ*	*(-) fakultativ*	(-)	(+)
Beispiel	Das Opfer wird vergewaltigt; der Täter oder eine dritte Person zeichnet die sexuellen Handlungen auf [und lädt die Daten auf eine Pornografieplattform hoch]	Das Opfer und der Partner haben einvernehmlichen Geschlechtsverkehr, der Sexualpartner zeichnet die Handlungen ohne Zustimmung des Opfers auf.	Das Opfer erstellt ein Nacktfoto von sich selbst und sendet es an den Partner; der Partner lädt es hoch, sog. „Revenge Porn“	Einvernehmliches Darstellen, Aufzeichnen und Veröffentlichen von pornografischem Material im Rahmen kommerzieller Pornografie
Datenbasierte sexuelle Gewalt	**ja**			**nein**
datenbasierte Handlung	ja			
sexuelle Konnotation / sexuelles Element	ja			
datenbasierte Elemente des Missbrauchs	ja (≥ 1)		ja	nein (vollständiges Einverständnis)

Legende:

kursiv / [Klammern] fakultative Komponenten

– – – – – – Schwellenwert: datenbasierte Elemente des Missbrauchs[79]

Bei Daten aus Cluster 2 hat der dargestellte sexuelle Akt tatsächlich nicht (so) stattgefunden. Die Schwelle für datenbasierte sexuelle Gewalt liegt jedoch jenseits dieser ersten Stufe.

79 Das erste Element des Missbrauchs – die nicht einvernehmliche sexuelle Handlung, die in den Daten dargestellt wird – ist nicht datenbasiert.

2. Eine sexuelle Konnotation

Das Element der sexuellen Konnotation setzt keine sexuelle Absicht seitens der dargestellten Person voraus. Maßgeblich ist vielmehr, dass der Inhalt aus der Perspektive des Täters sexualisiert wird. Ausreichend ist insoweit die Sexualisierung, sexuelle Objektivierung oder Fetischisierung durch den Täter (z.B. das Filmen einer Person in einer intimen, aber nicht per se sexuellen Situation wie beim Ausziehen, Duschen oder Toilettengang, um sexuelle Befriedigung für sich selbst oder andere zu erlangen). Entscheidend ist, ob sich dem datafizierten Inhalt nach seinem objektiven Erscheinungsbild in Verbindung mit den Umständen seiner Herstellung oder Verwendung eine sexualisierte Bedeutungszuschreibung entnehmen lässt. Diese kann sich namentlich aus dem Kontext der Aufnahme, der Auswahl oder Fokussierung bestimmter Körperbereiche, der Art der Präsentation oder der intendierten Nutzung ergeben. Damit wird zugleich deutlich, dass nicht jede Darstellung intimer Situationen automatisch eine sexuelle Konnotation aufweist. Erforderlich ist vielmehr, dass die Darstellung über die bloße Abbildung hinaus eine sexualisierte Perspektive vermittelt, die die dargestellte Person zum Objekt sexueller Betrachtung macht. Eine sexuelle Motivation fungiert insoweit als Auslegungshilfe, ist jedoch nicht zwingend erforderlich, sofern sich die Sexualisierung aus den Umständen hinreichend erschließen lässt.

3. Die Ausführung einer oder mehrerer Stufen mittels digitaler Technologie

Dies stellt die entscheidende Schwelle dar, die aus einem Verhalten *datenbasierte* sexuelle Gewalt macht. Bei Daten aus Cluster 1 betrifft dies die Erstellung (d.h. die Datenerfassung einer tatsächlich stattgefundenen Handlung) und/oder die Verbreitung solcher Daten. Bei Daten aus Cluster 2 ist es die Erstellung (d.h. die Fiktion oder verfälschende Darstellung einer Handlung) und/oder die Verbreitung dieser Daten.

Um das Ziel eines Strafrechts zu erreichen, das sowohl umfassend schützt als auch Rechte wie die Kunst- und Meinungsfreiheit[80] angemessen berücksichtigt, sind Abgrenzungen erforderlich. **Abstufungen** und Schweregrade müssen auf Grundlage der Umstände des Einzelfalls bestimmt werden, wobei die Einstufung von Daten als authentisch (Cluster 1) oder gefälscht (Cluster 2) ein entscheidender Faktor sein kann. Diese Differenzierung will nicht als opferbeschuldigend missverstanden werden (z.B. die allgemeine Betrachtung von DBSA-Handlungen als weniger schwerwiegend, wenn das Opfer die ohne Einwilligung verbreiteten Daten selbst erstellt hat). Vielmehr gilt: Je authentischer die Daten sind oder erscheinen, desto schwerwiegender ist die Rechtsverletzung. So ist etwa zu berücksichtigen, wenn ein Dee-

80 Zur kreativen/künstlerischen Wirkung besonders aufwendig inszenierter Pornografie im Gegensatz zu amateurhaften Aufnahmen s. *Andresen/Dreyer*, Online-Formen aufgezwungener Sexualität (Fn. 19), S. 3.

pfake-Video selbst für das ungeübte Auge leicht als Fälschung erkennbar ist; dies ist in die Interessenabwägung und die strafrechtliche Bewertung – jedenfalls i.H.a. Verletzungen der informationellen Selbstbestimmung durch Falschdarstellungen – einzubeziehen.

C. Aktuelle Rechtslage

Aufbauend auf der terminologischen Grundlage wird die aktuelle Rechtslage diskutiert, um mögliche Schutz- und Strafbarkeitslücken zu identifizieren.

I. Internationale Rechtsquellen

Die meisten digitalen Handlungen verbleiben nicht innerhalb der nationalen Grenzen des Landes, von dem aus sie begangen werden. Internationale Regelungen zur Prävention digitaler Kriminalität sind daher von entscheidender Bedeutung. Zu den EU-Rechtsvorschriften, die teilweise auf Cybergewalt anwendbar sind, gehören u.a. die Opferschutzrichtlinie (Richtlinie 2012/29/EU), die Richtlinie zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie (RL (EU) 2011/93/)[81] und die Datenschutz-Grundverordnung (VO (EU) 2016/679).[82] Spezifische Vorschriften zur Bildweitergabe[83] gibt es insbesondere in Bezug auf Material zum sexuellen Missbrauch von Kindern.[84]

Auf internationaler Ebene ist das Übereinkommen des Europarats zur Verhütung und Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt (sog. Istanbul-Konvention) ein wichtiger Rechtsrahmen, der teilweise auch für Cybergewalt gilt.[85] Gemäß Art. 3 lit. a bezeichnet der Begriff „Gewalt gegen Frauen" alle Handlungen geschlechtsspezifischer Gewalt, die zu (bspw. körperlichen, sexuellen, psychischen) Schäden oder Leiden bei Frauen führen (können). Angesichts ihrer geschlechtsspezifischen Ausprägung und Schädlichkeit[86] sind DBSA-Handlungen gegenüber Frauen als „Gewalt gegen Frauen" im Sinne der Istanbul-Konvention zu

81 Hierzu weiterführend *Schmidt*, Pornographie (Fn. 16), S. 206.

82 Einen Überblick bietet die *EIGE*-Studie (Fn. 68), S. 201 f. m.w.N.; vgl. auch djb e.V., Policy Paper: Digitale Gewalt (Fn. 74), S. 4 ff.

83 Vgl. *C. Walkey/K. Mantouvalou/N. Meurens/O. Kouaya/I. Pavlovaite*, The legislative frameworks for victims of gender-based violence (including children) in the 27 Member States, online abrufbar unter <https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2022)738126>, zuletzt abgerufen am 15.1.2026, S. 24.

84 Bilder, die als Material über sexuellen Kindesmissbrauch gelten, fallen unter die Richtlinie zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie (2011/93/EU), vgl. ebd.; darüber hinaus gibt es auf internationaler Ebene Rechtsquellen wie das Übereinkommen des Europarats zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch (sog. Lanzarote-Konvention, CETS No. 201), die den Missbrauch von Kindern, einschließlich bestimmter Formen von Cybergewalt, unter Strafe stellt, vgl. ebd., S. 22.

85 Vgl. auch djb e.V., Policy Paper: Digitale Gewalt (Fn. 74), S. 6 f.

86 Vgl. oben.

qualifizieren.[87] Darüber hinaus definiert Art. 40 sexuelle Belästigung als „jede Form von ungewolltem sexuell bestimmtem verbalem, nonverbalem oder körperlichem Verhalten mit dem Zweck oder der Folge, die Würde einer Person zu verletzen, insbesondere wenn dadurch ein Umfeld der Einschüchterung, Feindseligkeit, Erniedrigung, Entwürdigung oder Beleidigung geschaffen wird", und verpflichtet die Unterzeichnerstaaten, die erforderlichen gesetzgeberischen Maßnahmen zu ergreifen, um ein solches Verhalten unter Strafe zu stellen oder anderweitig zu sanktionieren. Diese Definition ist recht weit gefasst, da sie „jede Form" einschlägigen Verhaltens umfassen kann und somit generell alle Arten von DBSA abdeckt. Sie verweist zudem ausdrücklich auf die Einvernehmlichkeit des Verhaltens („ungewollt") und legt einen besonderen Schwerpunkt auf die daraus resultierende Rechtsgutsverletzung. Insbesondere mit Blick auf die Öffentlichkeit, die durch die Erstellung und/oder Verbreitung intimer Daten potenziell oder tatsächlich erzeugt wird, ist der in Art. 40 genannte Aspekt eines einschüchternden, feindseligen oder erniedrigenden Umfelds besonders relevant. Je nach Ebene und Ausprägung der DBSA-Handlung könnten bestimmte Erscheinungsformen gar als sexuelle Gewalt i.S.d. Art. 36 Abs. 1 lit. a der Istanbul-Konvention anzusehen sein: die Norm verpflichtet die Unterzeichnerstaaten, die erforderlichen Maßnahmen zu ergreifen, um „sonstige nicht einverständliche sexuell bestimmte Handlungen " unter Strafe zu stellen („sonstige" ist die Abgrenzung zu den in Art. 36 Abs. 1 lit. b genannten penetrativen sexuellen Handlungen). Einige Formen von DBSA, die mit Nötigung oder Bedrohung des Opfers verbunden sind, können auch als psychische Gewalt oder Stalking i.S.d. Art. 33 und 34 eingeordnet werden. Auch GREVIO hat in seinen ersten „General Recommendations" festgestellt, dass einige DBSA-Formen unter die Begriffe geschlechtsspezifischer Gewalt bzw. sexueller Belästigung i.S.d. Art. 3 lit. a), Art 40 IK fallen.[88]

Neben der Istanbul-Konvention ist auch das Budapester Übereinkommen über Computerkriminalität sowie sein Zusatzprotokoll zu berücksichtigen. Das Hauptziel des Übereinkommens ist der Schutz vor Cyberkriminalität durch die Schaffung einer gemeinsamen kriminalpolitischen Grundlage.[89]

87 Vgl. hierzu auch *C. Rigotti/C. McGlynn*, Criminalising Image-Based Sexual Abuse Across Europe: Seeking Comprehensive Legal Redress Reflecting Victims' Experiences, in: Burghardt et al. (Hrsg.), Sexuelle Selbstbestimmung (Fn. 27), S. 99 (100, 104 ff.).

88 GREVIO, General Recommendation No. 1 on the digital dimension of violence against women (20.10.2021), online abrufbar unter <https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147>, zuletzt abgerufen am 19.1.2026, vgl. Empfehlung Nr. 33 u.a. zum nicht-konsensuellen Teilen oder Verbreiten von Bildern oder Videos sowie Empfehlung Nr. 38 (a) und (b) zu „Revenge Porn" und „Deepfakes" als digitale sexuelle Belästigung. Vgl. auch *Schmidt*, Pornographie (Fn. 16), S. 205.

89 *EIGE*-Studie (Fn. 68), S. 22 m.w.N.

Hinzu kommt – jünger – die Richtlinie zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt (RL (EU) 2024/1385). Diese fordert in Art. 5 Abs. 1 die Kriminalisierung einiger vorsätzlicher DBSA-Handlungen. Hierzu gehören die nicht-einverständliche Zugänglichmachung für die Öffentlichkeit von Bild- oder vergleichbaren Daten, die sexuelle Handlungen oder intime Körperteile einer anderen Person darstellen, sofern diese Handlungen wahrscheinlich dazu führen, dass der betroffenen Person schwerer Schaden zugefügt wird (lit. a)) sowie die nicht-einverständliche Herstellung, Manipulation oder Veränderung von Bild- oder vergleichbaren Daten, die den Anschein erwecken, dass eine Person sexuelle Handlungen vornimmt, und deren anschließende Veröffentlichung (lit. b)). Auch die Androhung solcher Handlungen ist erfasst (lit. c)). Obgleich die Vorgaben i.H.a. die Tathandlungen i.E. keinen umfassenden Schutz bieten,[90] liegt hierin eine grundsätzliche, europarechtliche Anerkennung der Strafwürdigkeit einer Verletzung der Verfügungsbefugnis über persönliche, sexualbezogene Inhalte (als Ausfluss des Rechts auf sexuelle i.V.m. informationeller Selbstbestimmung).[91]

Darüber hinaus findet die EMRK teilweise Anwendung auf DBSA: So verbietet beispielsweise Art. 3 erniedrigende Behandlung; das Recht auf Achtung des Privat- und Familienlebens[92] wird durch Art. 8 gewährt.[93] Art. 10 gewährt die Meinungsfreiheit, die indes aus beiden Perspektiven betrachtet werden muss (vgl. hierzu unten C.III.).

Insgesamt bietet der internationale Rechtsrahmen zu digitaler Gewalt und – spezifischer – zu DBSA noch keinen umfassenden Bezugsrahmen und keine detaillierten Leitlinien. Obwohl die Istanbul-Konvention in Bezug auf DBSA nicht übermäßig spezifisch ist, enthält sie doch einige Verpflichtungen für die Unterzeichnerstaaten; es bleibt zu prüfen, ob das deutsche Strafrecht diesen Anforderungen entspricht.

II. Strafrechtliche Erfassung

Das deutsche Strafrecht enthält verschiedene Tatbestände zum Schutz der sexuellen Selbstbestimmung. Die §§ 184–184c StGB stellen die Verbreitung pornografischer Inhalte *an* bestimmte Empfänger:innen (insbesondere Minderjährige), die Verbreitung pornografischer Inhalte, die Gewalthandlungen oder sexuelle Handlungen mit Tieren *darstellen*, sowie die Verbreitung, Beschaffung und den Besitz von kinder- oder jugendpornografischen Inhalten unter Strafe. § 184 Abs. 1 Nr. 6 StGB erfasst das unaufgeforderte Zusenden pornografischer Inhalte an Erwachsene; das Versenden solcher Inhalte an Minderjährige unterfällt (zustimmungsunabhängig)

90 *Schmidt*, Pornographie (Fn. 16), S. 250.

91 Ebd., S. 206, 250.

92 Vgl. in diesem Zusammenhang z.B. *Volodina gegen Russland (Nr. 2)* (Fn. 52); *Buturugă gegen Rumänien* (Fn. 52).

93 *EIGE*-Studie (Fn. 68), S. 23 m.w.N.

schon § 184 Abs. 1 Nr. 1 StGB.[94] Das unaufgeforderte Zusenden eines sog. Dick Pics fällt nach teilweiser Auffassung jedoch nicht unter § 184 Abs. 1 Nr. 6 StGB, da die bloße Wiedergabe eines Genitals keinen pornografischen Inhalt i.S.d. Norm darstelle.[95] § 184k StGB wurde ausdrücklich im Hinblick auf die Phänomene „Upskirting" und „Downblousing" eingeführt.[96] Die Norm stellt die Herstellung und Übermittlung eines Fotos oder sonstigen Bildes intimer Körperteile (gem. § 184k Abs. 1 Nr. 1 StGB: die Genitalien, das Gesäß oder die weibliche Brust oder die diese Körperteile bedeckende Unterwäsche, soweit diese Bereiche gegen Anblick geschützt sind) unter Strafe. Der Gebrauch oder das Zugänglichmachen eines solchen Bildes an Dritte ist gem. § 184k Abs. 1 Nr. 2 StGB strafbar. Somit sind zwei prominente Arten von DBSA nach geltendem nationalem Strafrecht strafbar. Die §§ 183 und 183a StGB stellen beide im Wesentlichen exhibitionistische Handlungen unter Strafe. Die in § 183 StGB („Exhibitionistische Handlungen") normierte Tathandlung kann nur von einem männlichen Täter[97] begangen werden, während § 183a StGB („Erregung öffentlichen Ärgernisses") von jeder Person verwirklicht werden kann. Nach h.M. erfasst § 183 StGB nicht die Konfrontation anderer mit einer sexuellen Handlung mittels akustischer, schriftlicher oder visueller Daten, einer Bilddarstellung oder Live-Übertragungen (online); die Norm setzt vielmehr die gleichzeitige physische Anwesenheit von Täter:in und Opfer voraus.[98] DBSA-Handlungen fallen daher nicht unter § 183 StGB. Demgegenüber verlangt § 183a StGB die Vornahme einer sexuellen Handlung in der Öffentlichkeit unter Erregung eines Ärgernisses. „Cyber-Exhibitionismus" scheint diese Voraussetzungen auf den ersten Blick zu erfüllen. Die öffentliche Zurschaustellung von Fotos oder Filmen ist jedoch nicht die tatsächliche Vornahme der in § 183a StGB geforderten sexuellen Handlung,[99] und der Tatbestand erfasst auch nicht die „Veröffentlichung" der sexuellen Handlungen anderer Personen (z. B. durch heimliches Beobachtbarmachen) ohne oder gegen deren Willen.[100] §§ 183 f. StGB greifen da-

94 *A. Schmidt*, in: V. Erb/J. Schäfer (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 3, 5. Aufl., München 2025, § 184 Rn. 67; *Andresen/Dreyer*, Online-Formen aufgezwungener Sexualität (Fn. 19), S. 3 mit einer eingehenden Analyse und m.w.N.

95 *A. Schmidt*, in: Erb/Schäfer (Hrsg.), MüKo-StGB Bd. 3 (Fn. 94), § 184 Rn. 68, 19 ff.

96 § 184k StGB wurde durch das 59. StrÄndG vom 9.10.2020 (BGBl. I S. 2075) eingefügt. Zuvor hatten zivilgesellschaftliche Aktivist:innen auf das Thema aufmerksam gemacht und eine Kriminalisierung gefordert, siehe *Seidel/Sassenberg* (Fn. 60); *T. Mengler*, Strafwürdigkeit voyeuristischer ‚Upskirt'-Aufnahmen, ZRP 2019, S. 224 gibt einen Überblick über den Kontext der §§ 201, 201a und 184k StGB.

97 Zur Verfassungsmäßigkeit vgl. *A. Schmidt*, in: Erb/Schäfer (Hrsg.), MüKo-StGB Bd. 3 (Fn. 94), § 183 Rn. 6 m.w.N.

98 *T. Fischer*, Strafgesetzbuch mit Nebengesetzen, 72. Aufl., München 2025, § 183 Rn. 5; a.A. wohl *A. Schmidt*, in: Erb/Schäfer (Hrsg.), MüKo-StGB Bd. 3 (Fn. 94), § 183 Rn. 12, wonach das Zusenden sog. Dick Pics unter § 183 StGB fallen kann; die Tathandlung werde um die digitale Begehung erweitert.

99 *A. Schmidt*, in: Erb/Schäfer (Hrsg.), MüKo-StGB Bd. 3 (Fn. 94), § 183a Rn. 7.

100 *Fischer*, StGB (Fn. 98), § 183a Rn. 3 m.w.N.

her weder bei Cyber-Exhibitionismus noch bei datenbasierten Formen des Voyeurismus.

Datenbasierter Voyeurismus fällt indes – weitgehend[101] – unter die Vorschriften zur Verletzung des höchstpersönlichen Lebensbereichs und der Privatsphäre (§§ 201a, 202a ff. StGB). § 201a Abs. 1 Nr. 1 StGB stellt die unbefugte Herstellung oder Übertragung von Bildmaterial einer anderen Person in einer Wohnung oder in einem gegen Einblick besonders geschützten Raum unter Strafe, wenn dies den höchstpersönlichen Lebensbereich der abgebildeten Person verletzt. Der Gebrauch von Bildaufnahmen, die auf diese Art entstanden sind, oder deren Weitergabe an Dritte ist ebenfalls nach § 201a Abs. 1 Nr. 4 und Nr. 5 StGB strafbar. Somit sind neuere Formen des Voyeurismus durch das aktuelle deutsche Strafrecht abgedeckt. Deepfakes hingegen sind von § 201a StGB nicht erfasst, da es sich nicht um eine Bildaufnahme, sondern um einen „computertechnisch veränderten Bildinhalt" handelt.[102] Die §§ 202a bis 202d StGB stellen das Ausspähen und Abfangen von Daten (Phishing), damit zusammenhängende Vorbereitungshandlungen und Datenhehlerei unter Strafe. Das Beschaffen und/oder Beschaffenlassen, Bereitstellen oder Verbreiten gestohlener Daten (intimer oder anderer Art) ist nach diesen Normen also ebenfalls strafbar. Zu bedenken bleibt, dass sog. Rachepornos, die ursprünglich einvernehmlich geteilt und dann ohne Zustimmung weiterverbreitet wurden, nicht von diesen Tatbeständen erfasst sind.[103] Diese Art von DBSA kann jedoch gemäß § 184k Abs. 1 Nr. 3 StGB strafbar sein, wonach es verboten ist, Bildaufnahmen intimer Körperbereiche (wie in Nr. 1 beschrieben) ohne Einwilligung Dritten zugänglich zu machen, auch wenn das Bild ursprünglich einvernehmlich hergestellt wurde.[104] Schließlich kann die strafrechtliche Verantwortlichkeit einiger Arten von DBSA gemäß §§ 185 ff. (Beleidigung),[105] § 238 (Nachstellung)[106] oder § 240 StGB (Nötigung) sowie §§ 118, 119 OWiG[107] in Betracht kommen.

101 Eingehend *Sanow*, Voyeuristische Bildaufnahmen (Fn. 3), S. 100 ff.

102 djb e.V., Policy Paper: Rechtlicher Handlungsbedarf bei nicht-einvernehmlichen sexualisierenden Deepfakes (st26–09), Manuskript-S. 8 (im Erscheinen).

103 Nichts anderes ergibt sich schon aus dem Wortlaut der §§ 202a Abs. 1, 202b StGB („unbefugt"); vgl. auch *J. Graf*, in: V. Erb/J. Schäfer (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 4, 5. Aufl., München 2025, § 202a Rn. 65.

104 *J. Renzikowski*, in: Erb/Schäfer (Hrsg.), MüKo-StGB Bd. 3 (Fn. 94), § 184k Rn. 21.

105 Zu sexuellen Beleidigungen vgl. *P. Regge/C. Pegel*, in: Erb/Schäfer (Hrsg.), MüKo-StGB Bd. 4 (Fn. 103), § 185 Rn. 15 ff.; siehe auch *Andresen/Dreyer*, Online-Formen aufgezwungener Sexualität (Fn. 19), S. 4.

106 *Andresen/Dreyer*, Online-Formen aufgezwungener Sexualität (Fn. 19), S. 4; vgl. außerdem *J. Gericke*, in: Erb/Schäfer (Hrsg.), MüKo-StGB Bd. 4 (Fn. 103), § 238 Rn. 36 m.w.N.

107 *Andresen/Dreyer*, Online-Formen aufgezwungener Sexualität (Fn. 19), S. 45 f.

Insgesamt werden mehrere Formen von DBSA de lege lata nicht oder nicht umfassend abgedeckt.[108] Dies gilt insbesondere für Deepfakes,[109] veränderte oder KI-generierte Inhalte.[110] Zwar kann der Vergleich mit § 267 StGB[111] bei der Entwicklung neuer Regelungen für gefälschte Daten fruchtbar gemacht werden, doch existieren derzeit keine einschlägigen Strafnormen. Als *ultima ratio* muss das Strafrecht stets am Verhältnismäßigkeitsprinzip ausgerichtet werden, seine Notwendigkeit muss abgewogen und die Legitimation von Gesetzen reflektiert werden.[112] Die Vorgaben der Istanbul-Konvention könnten jedoch eine Verpflichtung zur Kriminalisierung einiger Arten von DBSA erfordern, die bisher noch nicht erfasst sind. Dies lässt sich insbesondere aus Art. 40 der Konvention ableiten.[113]

III. Zivilrechtliche Perspektiven

Das Strafrecht stößt gleichwohl dort an seine Grenzen, wo die ursprüngliche Rechtsgutsverletzung nicht mehr nur durch individualisierbare Einzeltäter*innen bewirkt wird, sondern vielmehr durch „die Öffentlichkeit". Die strafrechtliche Verfolgung der Person, die beispielsweise „Revenge Porn" online gestellt hat, ist für die Betroffenen oft keine ausreichende Konsequenz, da die Rechtsgutsverletzung fortbesteht, solange das Bildmaterial im Internet abrufbar ist. Selbst eine erfolgreiche zivilrechtliche Inanspruchnahme des originären Täters auf Schadensersatz oder Unterlassung[114] vermag die Rechtsverletzung dann nur bedingt ein- und aufzufangen. Angesichts der Geschwindigkeit, mit der Inhalte online abgerufen, geteilt, gespeichert und erneut hochgeladen werden, ist deren vollständige Löschung nahezu unmöglich.[115] Daten, die in den schnell fließenden Strom des „Viralgehens" geraten sind, können sekündlich von Zehntausenden, wenn nicht

108 Ebd., S. 6 mit derselben Schlussfolgerung; vgl. auch *Clemm*, Digitale Gewalt (Fn. 38), S. 130.

109 So auch djb e.V., Policy Paper: Digitale Gewalt (Fn. 74), S. 9 ff. zu bestehenden Schutzlücken im nationalen Straf- und Zivilrecht; nach *J. Blocher*, Strafbare Deepfakes (Fn. 10), S. 227 ist das Strafrecht beim Schutz vor unechten Medieninhalten allgemein fragmentarisch und unübersichtlich. Vgl. zudem djb e.V., Policy Paper: Deepfakes (Fn. 102), Manuskript-S. 6 ff., 9 ff.

110 So auch *Beck/Nussbaum*, KI ohne Verantwortung (Fn. 35); ähnl. *Sanow*, Voyeuristische Bildaufnahmen (Fn. 3), S. 203; djb e.V., Stellungnahme zum geplanten „Digitalen Omnibus Paket" der Europäischen Kommission, Manuskript-S. 9 f. (im Erscheinen) zu Schutzlücken auch mit Blick auf geplante Regelungen.

111 Siehe oben.

112 *J. Renzikowski*, in: H. Matt/J. Renzikowski (Hrsg.), Strafgesetzbuch Kommentar, 2. Aufl., München 2020, Einleitung. Das strafrechtliche Programm Rn. 5; *V. Erb*, in: V. Erb/J. Schäfer (Hrsg.), Münchener Kommentar zum StGB, Bd. 1, 5. Aufl., München 2025, Einleitung Rn. 22 f.; vgl. weiterführend auch BVerfGE 64, 67.

113 *C. Rigotti/C. McGlynn/F. Benning*, Image-Based Sexual Abuse and EU Law: A Critical Analysis, German Law Journal 2024, 1472 (1479 f.) m.w.N.

114 Vgl. zu einem Schadensersatzanspruch aus § 823 BGB etwa *V. Kraetzig*, Deliktsschutz gegen KI-Abbilder – Teil 1: Täuschende Deepfakes, CR 2024, S. 207 (210 ff.); *Sanow*, Voyeuristische Bildaufnahmen (Fn. 3), S. 173 ff.; zu einem Unterlassungsanspruch aus § 1004 BGB analog ebd., S. 180 ff.; allg. zu Möglichkeiten der Abmahnung, Unterlassung oder einstweiligen Verfügung *Dinig*, Zivilrechtliche Interventionen (Fn. 37), S. 152 ff.

115 So auch *EIGE*-Studie (Fn. 68), S. 52 m.w.N.

Hunderttausenden von Nutzern angesehen werden. Selbst wenn Daten sich nicht „viral" verbreiten, gibt es nach dem Hochladen keine Möglichkeit, ihre vollständige und dauerhafte Löschung zu gewährleisten. Es gibt ganze Websites, die sich der Archivierung von Online-Inhalten[116] oder gar explizit der Sammlung von „Revenge Porn"[117] widmen.

(Auch) der Fall der Grünen-Politikerin *Renate Künast*[118] zeigte eindrucksvoll, dass das materielle Strafrecht allein zur effektiven Verfolgung digitaler Straftaten nicht ausreicht. Die Vorfälle betrafen Hasskommentare und Beleidigungen, die von anonymen Nutzern auf Social-Media-Plattformen veröffentlicht worden waren. *Künast* hatte vom Plattformbetreiber (Facebook) die Herausgabe der Nutzerdaten verlangt, um rechtliche Schritte gegen sie einzuleiten. Die Zivilgerichte lehnten zunächst eine Pflicht zur Herausgabe dieser Daten ab,[119] wodurch es *Künast* praktisch unmöglich war, rechtliche Schritte gegen die anonymen Urheber der Beleidigungen einzuleiten.

Der Anreiz für Anbieter, individuelle Rechte zu schützen, ist gering. Der „Digital Service Act" (DSA)[120] enthält etwa in Art. 6 einen Haftungsausschluss für Hosting-Dienste (Provider), „um die Haftungsrisiken für diese Dienste zu minimieren".[121] Plattformbetreiber sind aufgrund der Haftungsprivilegierung in Art. 6 Abs. 1 lit. a DSA (Umsetzung über § 7 Abs. 1 DDG) nicht zu einer aktiven Überwachung sämtlicher Inhalte verpflichtet.[122] Eine Haftung besteht gem. Art. 6 Abs. 1 lit. b DSA auch nicht, wenn der Diensteanbieter die rechtswidrigen Inhalte infolge einer Mitteilung zügig sperrt oder diese entfernt. Auch ein Schadensersatzanspruch aus Art. 82 Abs. 1 DSGVO wird angesichts der Exkulpationsmöglichkeit aus Abs. 3 der Norm praktisch wohl häufig keine Grundlage für Betroffene bilden, gegen Provider vorzugehen.

116 Vgl. etwa das „Internet Archive", eine US-amerikanische Non-Profit-Website, die sich der Archivierung digitaler Medien verschrieben hat, online abrufbar unter < https://archive.org/>, zuletzt abgerufen am 9.1.2026.

117 Vgl. ausführl. *C.A. Uhl/K.J. Rhyner/C.A. Terrance/N.R. Lugo*, An examination of nonconsensual pornography websites, Feminism & Psychology 2018, S. 50.

118 Das langwierige Verfahren wurde medial intensiv begleitet und löste Diskussionen über die Schwellen der Ehrverletzungsdelikte, Hinnahmepflichten von Politiker:innen bzw. Personen des öffentlichen Lebens und über die Verantwortlichkeit von Plattformbetreibern aus. Die Gerichtsentscheidungen stießen in der Literatur auf Kritik; vgl. etwa *D. Höch*, Der ‚Künast-Beschluss' zu Schmähkritik: rechtlich nicht haltbar und schädlich für die Demokratie, Kommunikation & Recht 2019, S. 680; *Regge/Pegel* (Fn. 105), § 185 Rn. 12.

119 Im Mittelpunkt stand § 14 Abs. 3 i.V.m. § 1 Abs. 3 des Telemediengesetzes (TMG) in seiner alten Fassung.

120 Verordnung (EU) 2022/2065.

121 OLG Frankfurt a.M. GRUR-RS 2025, 3551 Rn. 12.

122 *C. Bildhäuser*, Aktuelle Entwicklungen der Rechtsprechung zur Haftung von Plattformen für Deep Fakes nach Digital Services Act, GRUR-Prax 2025, 480, 481; OLG Frankfurt a.M. GRUR-RS 2025, 3551 Rn. 9; zu der Haftungsprivilegierung differenzierend nach Plattformen und LLMs *Beck/Nussbaum*, KI ohne Verantwortung (Fn. 35).

Im Fall *Künast* hob das Bundesverfassungsgericht die vorinstanzlichen Urteile schließlich auf.[123] Dennoch ist der enorme zeitliche und finanzielle Aufwand zu berücksichtigen, den *Künast* investieren musste. Rechtsschutz gegen digitale Gewalt war und ist in vielen Fällen ein komplexes und kostspieliges Unterfangen.[124] Insgesamt zeigt sich, dass auch zivilrechtliche Ansprüche in der Praxis häufig leerlaufen.[125] Die Urheber der übergriffigen Inhalte bleiben im Internet anonym, die Rechtspraxis ist überfordert, die Plattformbetreiber kooperieren kaum. In diesem Zusammenhang müssen die (bspw. finanzielle) Sanktionierung und Haftung von Anbietern[126] sowie die übergeordnete Frage der strafrechtlichen Haftung von Unternehmen weitergehend diskutiert werden, was jedoch den Rahmen dieses Beitrags übersteigt.

IV. Digitale sexualisierte Gewalt im Spannungsfeld zwischen Opferrechten und Meinungsfreiheit

Neben den (straf- und zivil-)rechtspraktischen Erwägungen steht ein ewiger Interessenskonflikt. Das OLG Frankfurt a.M. stellte jüngst wieder deutlich, dass die Feststellung einer Verletzung von Persönlichkeitsrechten eine Abwägung zwischen den Rechten der betroffenen Person aus Art. 1 Abs. 1, 2 Abs. 1 GG, Art. 8 Abs. 1 EMRK und dem Recht jedenfalls des Providers auf Meinungs- und Medienfreiheit (Art. 5 Abs. 1 GG, Art. 10 EMRK) erfordert.[127] Zwar müssen die jeweiligen Interessen sorgfältig gegeneinander abgewogen werden;[128] jedoch wird häufig nicht berücksichtigt, dass Betroffene, die durch Cybergewalt effektiv aus dem öffentlichen digitalen Raum verdrängt werden, ebenfalls in ihren Freiheiten eingeschränkt werden: der geschlechtsspezifische[129] „silencing effect“ kann die Teilhabe Betroffener an politischen und medialen Prozessen oder die Ausübung öffentlicher Ämter beeinträchtigen und sogar verhindern.[130] Die Herstellung eines Gleichgewichts zwischen Meinungsfreiheit und Zensurrisiken einerseits, effektivem Schutz der sexuellen und informationellen Selbstbestimmung andererseits erfordert eine kontext- und machtsensible Abwägung, die strukturelle Ungleichheiten, digitale Verbrei-

123 BVerfG NJW 2022, 680.

124 Vgl. zum Kostenrisiko und zur Darlegungspflicht (aufgrund fehlenden Amtsermittlungsgrundsatzes im Zivilrecht) auch *Dinig*, Zivilrechtliche Interventionen (Fn. 37), S. 156; *Sanow*, Voyeuristische Bildaufnahmen (Fn. 3), S. 192 f.

125 Zu Auskunftsansprüchen und den praktischen Problemen in der zivil- und strafrechtlichen Verfolgung s. etwa *Clemm*, Digitale Gewalt (Fn. 38), S. 141 ff.

126 Krit. zur Ausrichtung geplanter Regelungen auch djb e.V., Stellungnahme (Fn. 110), S. 10 sowie djb e.V., Policy Paper: Digitale Gewalt (Fn. 74), S. 13.

127 OLG Frankfurt a.M. GRUR-RS 2025, 3551 Rn. 10.

128 Vgl. etwa zum legitimen Interesse an Anonymität im Netz *Clemm*, Digitale Gewalt (Fn. 38), S. 141.

129 Siehe auch *Crone*, Pornografische Deepfakes (Fn. 34).

130 Vgl. hierzu *Moolman/Kamran/Smith*, Freedom of Expression (Fn. 53), insb. S. 8 f.; *EIGE*-Studie (Fn. 68), S. 52; *Almenar*, Cyber Violence (Fn. 75), S. 181.

tungsdynamiken und die faktische Reichweite von Eingriffen in die sexuelle und informationelle Selbstbestimmung berücksichtigt. Gleichermaßen müssen datenschutzrechtliche Reformentwürfe auch vor diesem Hintergrund geschlechtsspezifischer Viktimisierungsrisiken sorgfältig abgewogen werden, um bestehende Schutzlücken zu schließen und die Schaffung neuer zu verhindern.[131]

D. Fazit und Ausblick

Insbesondere mit dem neueren § 184k StGB sind einige DBSA-bezogene Rechtsgutsverletzungen aus Cluster 1 – theoretisch – bereits strafbar. Auch im Zivilrecht gibt es eine Reihe an Anspruchsgrundlagen zugunsten Betroffener. Dennoch bestehen berechtigte Zweifel an der Effektivität der Vorschriften in der Rechtspraxis.[132] Gemeinsamer Nenner der straf- und zivilrechtlichen Problemstellungen ist die Verselbstständigung und Unkontrollierbarkeit der Datafizierung – mit anderen Worten: die Datenmengen sind zu groß für Einzelfallgerechtigkeit.

Der Beitrag zeigt die Notwendigkeit der Anerkennung bestimmter Formen der *daten*basierten und nicht nur der bildbasierten sexuellen Gewalt. Die Analysen verdeutlichen, dass eine Reihe von DBSA-Verhaltensweisen bereits durch das geltende deutsche Strafrecht abgedeckt sind, teils aber kleinteilig und unsystematisiert von Einzelvorschriften erfasst werden, deren aktuell diskutierte weitere Ergänzung deshalb auch kaum tragfähig ist.[133] Es bestehen derzeit Lücken und erhebliche Schutzdefizite sowohl im materiellen Strafrecht als auch – insbesondere – in der strafrechtlichen Praxis. Nichts anderes gilt im Zivilrecht. Und es bleibt offen, ob das materielle Recht ausgebaut werden oder ob zweckmäßigere verfahrensrechtliche (Ermittlungs-)Maßnahmen eingeführt werden müssen. In jedem Fall ist gesetzgeberisches Handeln erforderlich. Doch – und das hat der Beitrag gezeigt – erlaubt die Vielschichtigkeit von DBSA eben keinen einseitigen, einzelne Vorschriften erweiternden, Ansatz. Erforderlich ist vielmehr ein ganzheitliches Maßnahmenkonzept, das etwa die Aufklärung und Sensibilisierung der Nutzer:innen über Risiken und Präventionsmöglichkeiten (auch schon als Früherziehung) umfasst, sowie die

131 Vgl. zum sog. "Digital-Omnibus" *A. Ströbele Romero*, Daten-Omnibus der EU: Staaten halten an der DSGVO fest, Tagesspiegel Background vom 24.2.2026, online abrufbar unter <https://background.tagesspiegel.de/digitalisierung-und-ki/briefing/staaten-halten-an-der-dsgvo-fest>, zuletzt abgerufen am 27.2.2026; krit. zu Schutzlücken djb e.V., Omnibus-Stellungnahme (Fn. 104).

132 So auch djb e.V., Policy Paper: Digitale Gewalt (Fn. 74), S. 12 f. mit entsprechenden Verbesserungsvorschlägen.

133 Deutlich *A. Kaufmann*, Reform des Sexualstrafrechts. Dieser Gesetzentwurf zerlegt Frauen in ihre Einzelteile, in: Legal Tribune Online v. 31.03.2026, online abrufbar unter <https://www.lto.de/persistent/a_id/59634>, zuletzt abgerufen am 06.04.2026. Zur geplanten Ergänzung von § 184k StGB durch den ministeriellen Entwurf vgl. die auf netzpolitik.org geteilte Fassung zur weiteren nur detaillierten, kleinteiligen Erweiterung. Demgegenüber bereits strukturell im hier vorgeschlagenen Sinne ein am 24.3.2026 vorgelegter Vorschlag der Abgeordneten L. Gumnior, H. Limburg, T. Steffen, L. Benner, A. Tesfaiesus, F. Brantner, S. Schmidt und der Fraktion BÜNDNIS 90/DIE GRÜNEN, BT-Drs. 21/4949, S. 6.

Entwicklung von Schutzinstrumenten und technischen Lösungen für Social-Media-Plattformen.

Die Möglichkeiten für missbräuchliches Verhalten sind ebenso vielfältig und weitreichend wie die heutige Internetlandschaft. Die Kombination aus missbräuchlichem Verhalten jeglicher Art, Datafizierung und einer sexuellen Komponente ist besonders gefährlich; ihr Unrechtsgehalt unterscheidet sich von anderen Straftaten und stellt eine spezifische Form datenbasierter Gewalt dar: es bedarf grundsätzlich des Schutzes gegen unbefugt sexualisierte Datafizierung.[134] Zwar ist die menschliche Kommunikation außerhalb von Rechtsgeschäften nicht völlig ungeschützt, dennoch bestehen im Bereich der sexuellen Kommunikation nach wie vor erhebliche Schutzlücken. Daher sind Rechtssysteme und politische Akteure weltweit aufgefordert, insbesondere den Schutz intimer Daten sicherzustellen. Der Schutz personenbezogener Daten, die die Sexualität einer Person betreffen, muss in politischen Prozessen priorisiert werden. Im deutschen Strafrecht ist es dabei besonders wichtig, die Lücke im Umgang mit (KI-)veränderten oder (KI-)generierten Inhalten zu schließen. Hier können strukturell ebenfalls bestehende Straftatbestände der Urkundenfälschung (§ 267 StGB) als Blaupause dienen und etwa in Gestalt eines § 201 b StGB[135] umgesetzt werden.

134 In diese Richtung auch *Kaufmann*, Reform des Sexualstrafrechts (Fn. 133).

135 So der Vorschlag des aktuellen Regierungsentwurfs laut netzpolitik.org mit einem neu einzufügenden § 201 b StGB. Der dortige Regelungsvorschlag geht allerdings in eine andere Richtung, wenn danach bestraft werden soll, wer den „Anschein erweckt, ein tatsächliches Geschehen in Bezug auf eine andere Person wiederzugeben, und der geeignet ist, dem Ansehen dieser Person erheblich zu schaden, unbefugt zugänglich macht“ (Auszug). Auch hier setzt der Entwurf einen lediglich kleinteiligen Regelungsansatz ohne systematische Struktur fort.