Bund Deutscher Kriminalbeamter

BDK |Wollankstraße 135|D-13187Berlin

Bundesministerium der Justiz und für Verbraucherschutz
Anton-Wilhelm-Amo-Str. 37
10117 Berlin

per Mail: digitalegewalt@bmjv.bund.de

Bundesvorsitzender

Ansprechpartner/in: Dirk Peglow
Funktion: Bundesvorsitzender

E-Mail: dirk.peglow@bdk.de
Telefon: +49 30 2463045-0

Datum: 23.05.2026

Stellungnahme des Bund Deutscher Kriminalbeamter e.V. (BDK) zum Referentenentwurf eines Gesetzes zur Stärkung des zivilrechtlichen und strafrechtlichen Schutzes vor digitaler Gewalt, Geschäftszeichen: IIIB7-611722#00002#0027 unter besonderer Berücksichtigung des parallel geführten Gesetzgebungsverfahrens zur Speicherung und Nutzung von IP-Adressdaten

Der BDK begrüßt die Zielrichtung des Entwurfs zur Stärkung des zivilrechtlichen und strafrechtlichen Schutzes vor digitaler Gewalt. Zugleich macht die Stellungnahme deutlich, dass der Entwurf nicht isoliert bewertet werden kann, sondern im Zusammenhang mit dem parallel geführten Vorhaben zur Speicherung und Nutzung von IP-Adressdaten betrachtet werden muss. Beide Vorhaben prägen gemeinsam die künftige Architektur digitaler Identifizierung.

Aus kriminalpolizeilicher Sicht stehen dabei vier Punkte im Vordergrund: die Vermeidung von Wertungsbrüchen zwischen zivilrechtlicher und strafprozessualer Identifizierung, die rechtssichere Verwertbarkeit zivilgerichtlich erlangter Provider-Daten, die praktische Begrenztheit einer Identifizierung allein über IP-Daten sowie die hinreichende Bestimmtheit neuer Straftatbestände bei KI-generierten Inhalten und technikgestützter Überwachung.

1. Gegenstand und Einordnung der Stellungnahme

Diese Stellungnahme bezieht sich primär auf den vom Bundesministerium der Justiz vorgelegten Referentenentwurf eines Gesetzes zur Stärkung des zivilrechtlichen und strafrechtlichen Schutzes vor digitaler Gewalt, im Folgenden: Entwurf „digitale Gewalt“. Ergänzend werden die kriminalfachlichen, strafprozessualen und systematischen Auswirkungen des parallel geführten Gesetzgebungsverfahrens zur Speicherung und Nutzung von IP-Adressdaten berücksichtigt.

Nach aktuellem Stand wurde der Entwurf zur IP-Adressspeicherung nach Abschluss der Ressortabstimmung und Verbändeanhörung vom Bundeskabinett beschlossen und in das parla-

mentarische Verfahren eingebracht. Er befindet sich derzeit in der frühen Befassung des Bundesrates, bevor die weitere parlamentarische Beratung im Bundestag erfolgt.

Diese parallele Gesetzgebung ist für die kriminalfachliche Bewertung des Entwurfs „digitale Gewalt“ von zentraler Bedeutung. Beide Regelungskomplexe greifen auf dieselbe technische Grundlage zurück: die nachträgliche Zuordnung von IP-Adressen zu Anschlussinhabern beziehungsweise zu konkreten Nutzerinnen und Nutzern. Gerade diese Zuordnung ist in vielen digitalen Deliktskonstellationen der erste und häufig entscheidende Schritt, um aus einem anonymen oder pseudonymen digitalen Verhalten eine verantwortliche Person bestimmen zu können.

Der BDK begrüßt grundsätzlich, dass der Gesetzgeber die Handlungsfähigkeit des Rechtsstaates im digitalen Raum stärken will. Zugleich ist darauf zu achten, dass die entstehende Gesamtarchitektur digitaler Rechtsdurchsetzung in sich stimmig, praxistauglich und verfassungsrechtlich tragfähig ausgestaltet wird.

2. Ausgangslage: Digitalisierung der Kriminalität und Ermittlungsrealität

Die Verlagerung strafrechtlich relevanter Verhaltensweisen in digitale Kommunikationsräume hat in den vergangenen Jahren zu einer strukturellen Veränderung der Ermittlungsrealität geführt. Dies betrifft insbesondere Deliktsbereiche wie Beleidigung, Bedrohung, Nachstellung, bildbasierte Persönlichkeitsrechtsverletzungen, digitale Einschüchterung, Identitätsmissbrauch sowie manipulative oder KI-generierte Inhalte.

Die kriminalpolizeiliche Praxis zeigt, dass sich diese Delikte häufig durch hohe Geschwindigkeit, Anonymisierung, kurzlebige Nutzerkonten, Plattformwechsel, internationale Anbieterstrukturen und eine oftmals fehlende unmittelbare Identifizierbarkeit der handelnden Personen auszeichnen. Inhalte können innerhalb kürzester Zeit verbreitet, gelöscht, gespiegelt oder auf andere Dienste verlagert werden. Für Betroffene entsteht dadurch nicht selten der Eindruck, dass der Rechtsstaat im digitalen Raum nur verzögert oder unzureichend handlungsfähig ist.

Der Erfolg strafrechtlicher und zivilrechtlicher Rechtsdurchsetzung hängt in diesen Fällen in besonderem Maße davon ab, ob verlässliche technische Zuordnungsdaten rechtzeitig vorhanden sind. IP-Adresse, Portnummer, Zeitstempel und Zeitzonenangabe sind dabei keine bloßen technischen Randinformationen. Sie sind in vielen Fällen die notwendige Voraussetzung dafür, einen digitalen Angriff einer Person zuordnen zu können.

Vor diesem Hintergrund reagieren die beiden Gesetzgebungsvorhaben auf zwei unterschiedliche, jedoch eng miteinander verbundene Regelungsprobleme. Der Entwurf „digitale Gewalt“ will Betroffenen bessere zivilrechtliche Möglichkeiten zur Identifizierung und Rechtsdurchsetzung eröffnen und zugleich strafrechtliche Schutzlücken schließen. Der Entwurf „IP-Adressspeicherung“ soll demgegenüber die technische Grundlage verbessern, damit IP-Adressen innerhalb eines begrenzten Zeitraums Anschlussinhabern zugeordnet werden können. Beide Vorhaben sind daher funktional miteinander verbunden und sollten auch gesetzgeberisch zusammen betrachtet werden.

3. Gesamtsystem der digitalen Rechtsdurchsetzung

Die beiden Gesetzgebungsvorhaben führen faktisch zu einer zweigeteilten Struktur der digitalen Identifizierung.

Zum einen sieht der Entwurf zur IP-Adressspeicherung die Einführung einer befristeten Speicherung von IP-Zuordnungsdaten durch Telekommunikationsdienste vor. Der Zugriff im Strafverfahren soll über die hierfür vorgesehenen strafprozessualen Befugnisse erfolgen, insbesondere im Umfeld des § 100g StPO. Diese Befugnisse sind an gesetzliche Voraussetzungen, gerichtliche Kontrolle, Erforderlichkeit und Verhältnismäßigkeit gebunden. Dabei differenziert das Strafprozessrecht nach Deliktsart, Gewicht der Straftat, Art der Kommunikation und Zweck der Datenerhebung. Die Regelung ist daher nicht allein auf den Bereich schwerster Kriminalität reduziert, sie bleibt aber bewusst in ein differenziertes strafprozessuales Eingriffssystem eingebettet.

Zum anderen eröffnet der Entwurf „digitale Gewalt“ zivilrechtliche Auskunfts- und Sicherungsmechanismen. Diese sollen Betroffenen ermöglichen, zur Durchsetzung zivilrechtlicher Ansprüche Auskunft über die Identität rechtsverletzender Nutzerinnen und Nutzer zu erhalten. Erfasst werden sollen dabei auch technische Zuordnungsdaten wie IP-Adresse, Portnummer und Zugriffszeitpunkt.

Beide Systeme greifen damit auf dieselbe technische Realität zurück. Sie unterscheiden sich jedoch erheblich hinsichtlich ihrer prozessualen Einbettung, ihrer Eingriffsschwellen und ihrer institutionellen Zuständigkeit. Das ist nicht per se unzulässig, bedarf aber einer ausdrücklichen gesetzgeberischen Begründung. Der BDK sieht hier einen zentralen Prüfungsbedarf.

4. Strukturelle Schieflage der Identifizierungsarchitektur

In der Gesamtschau entsteht eine funktionale Differenzierung zwischen strafprozessualer und zivilrechtlicher Identifizierbarkeit, die nicht auf einer ausdrücklich erkennbaren gesetzgeberischen Gesamtentscheidung beruht, sondern sich aus dem Zusammenspiel beider Regelungskomplexe ergibt.

Während der strafprozessuale Zugriff auf IP-Zuordnungsdaten an spezifische Eingriffsschwellen, Anordnungsvoraussetzungen und Verhältnismäßigkeitsprüfungen gebunden bleibt, eröffnet das zivilrechtliche Verfahren nach dem Entwurf „digitale Gewalt“ einen eigenständigen Weg zur Identifizierung digitaler Kommunikationsakteure. Diese Konstellation kann dazu führen, dass in bestimmten Fallgestaltungen eine Identifizierung im zivilrechtlichen Verfahren gelingt, während eine entsprechende Identifizierung im strafprozessualen Verfahren wegen der dort geltenden Voraussetzungen unterbleibt.

Der BDK bewertet dies nicht als zwingenden unauflösbaren Widerspruch. Zivilrechtliche Rechtsdurchsetzung und strafprozessuale Ermittlungsmaßnahmen verfolgen unterschiedliche Zwecke und sind verfahrensrechtlich unterschiedlich ausgestaltet. Das zivilrechtliche

Auskunftsverfahren soll Betroffenen helfen, eigene Ansprüche geltend zu machen. Das Strafverfahren dient der staatlichen Strafverfolgung. Gleichwohl greifen beide Wege auf dieselben technischen Identifizierungsdaten zurück und berühren dieselben grundrechtlichen Schutzbereiche. Der BDK sieht deshalb eine klärungsbedürftige Wertungsinkongruenz. Der Gesetzgeber sollte ausdrücklich begründen, weshalb bei derselben Ausgangstat eine Identifizierung über IP-Zuordnungsdaten im zivilrechtlichen Verfahren unter Umständen leichter erreichbar sein kann als im strafprozessualen Verfahren. Dabei muss vermieden werden, dass faktisch ein Ausweich- oder Umgehungseffekt entsteht. Was dem Staat im Strafverfahren aus Gründen der Verhältnismäßigkeit nur unter bestimmten Voraussetzungen möglich ist, sollte nicht ohne tragfähige Begründung über den zivilrechtlichen Weg deutlich niedrigschwelliger erreichbar sein.

5. Beispielszenario zur Veranschaulichung

Zur Verdeutlichung dieser systemischen Konstellation sei ein typischer Fall der digitalen Praxis dargestellt.

Eine Person wird über eine Social-Media-Plattform beleidigt. Strafrechtlich steht eine Beleidigung gemäß § 185 StGB im Raum. Die betroffene Person erstattet Strafanzeige und möchte wissen, wer hinter dem Account steht.

Im strafprozessualen Verfahren hängt die Identifizierung davon ab, welche Daten bei welchem Anbieter vorhanden sind, welche strafprozessuale Befugnis einschlägig ist und ob die gesetzlichen Voraussetzungen der Datenerhebung im konkreten Fall vorliegen. Gerade bei einfachen Ehrdelikten kann die Identifizierung über Verkehrsdaten in der Praxis an strafprozessualen Schwellen, an fehlenden gespeicherten Daten oder an der Verhältnismäßigkeitsprüfung scheitern.

Denn gemäß § 100g Abs. 2 StPO-E ist in den Fällen, in denen kein Verdacht einer Straftat von auch im Einzelfall erheblicher Bedeutung vorliegt, die Erhebung von Verkehrsdaten nur unter den übrigen Voraussetzungen des Absatzes 1, insbesondere Erforderlichkeit und Verhältnismäßigkeit im engeren Sinne, hinsichtlich einer mittels Telekommunikation begangenen Straftat zulässig.

Diese Einschränkungen gelten jedoch nicht in gleicher Weise, wenn eine Auskunft über Daten nach § 2 des Gesetzes gegen digitale Gewalt beantragt und erteilt wird. Da diese Daten nach § 3 Abs. 4 des Gesetzes gegen digitale Gewalt auch an Strafverfolgungsbehörden übermittelt werden dürfen, kann in der praktischen Folge der Eindruck entstehen, dass Privatpersonen über das zivilrechtliche Verfahren weitergehende oder jedenfalls leichter zugängliche Identifizierungsmöglichkeiten erhalten als die Strafverfolgungsbehörden, die an die strafprozessualen Zugriffsschwellen gebunden sind.

Damit stellt sich zugleich die Frage der Verwertbarkeit zivilgerichtlich erlangter Provider-Daten in anschließenden oder parallelen Strafverfahren. Der Entwurf erlaubt eine Übermittlung an Strafverfolgungsbehörden, klärt aber nicht hinreichend, unter welchen Voraussetzungen diese Daten im Strafverfahren verwertet werden dürfen und welche Anforderungen an Dokumentation, Zweckbindung, Datenintegrität und Rechtsschutz zu stellen sind. Der BDK regt daher eine

ausdrückliche gesetzgeberische Klarstellung an, damit zivilgerichtlich gesicherte Daten nicht später wegen ungeklärter Verfahrensfragen an Beweiswert verlieren.

Parallel hierzu kann die betroffene Person nach dem Entwurf „digitale Gewalt“ ein zivilgerichtliches Auskunftsverfahren betreiben. In diesem Verfahren kann das zuständige Gericht gegenüber Diensteanbietern und Internetzugangsanbietern die Sicherung und Herausgabe von Daten anordnen, die zur Identifizierung erforderlich sind. Dazu können insbesondere IP-Adresse, Portnummer, Zeitpunkt des Zugriffs und eine Kopie des angegriffenen Inhalts gehören.

In der praktischen Folge kann die Identifizierung einer Person wegen einer Beleidigung im zivilrechtlichen Verfahren einfacher erreichbar sein als im Strafverfahren. Der BDK hält es für erforderlich, diese Schnittstelle ausdrücklich gesetzgeberisch zu prüfen und zu begründen. Es geht dabei nicht darum, Betroffenen den zivilrechtlichen Weg zu versperren. Es geht darum, die Gesamtarchitektur stimmig auszugestalten und Wertungsbrüche zwischen Strafverfolgung und privater Rechtsdurchsetzung zu vermeiden.

6. Zivilrechtliche Konstruktion, Accountsperren und Belastungsverschiebung

Der Entwurf „digitale Gewalt“ verlagert wesentliche Elemente der Identifizierung digitaler Rechtsverletzer in zivilgerichtliche Verfahren. Damit werden insbesondere Landgerichte mit technisch und organisatorisch komplexen Fragen befasst, die bislang häufig im Kontext strafprozessualer Ermittlungen durch spezialisierte Ermittlungsbehörden bearbeitet wurden.

Dies betrifft die Zuordnung von IP-Adressen, die Bedeutung von Portnummern, die Genauigkeit von Zeitstempeln, Plattformarchitekturen, internationale Datenverarbeitungsstrukturen, Anbieterreaktionen und die Frage, welche technischen Angaben für eine belastbare Identifizierung ausreichen. Der BDK sieht darin kein grundsätzliches Argument gegen ein zivilrechtliches Auskunftsverfahren. Für Betroffene kann ein eigener, gerichtlicher Weg zur Identifizierung ein wichtiger Fortschritt sein. Allerdings sollte der Gesetzgeber realistisch berücksichtigen, dass damit neue Anforderungen an die Zivilgerichte entstehen. Es geht nicht lediglich um einfache Auskunftsbeschlüsse, sondern um technisch anspruchsvolle und häufig eilbedürftige Verfahren.

Hinzu kommt die im Entwurf vorgesehene Möglichkeit, in gravierenden Fällen die Sperrung von Nutzerkonten gerichtlich anordnen zu lassen. Auch dies kann aus Sicht des BDK ein sinnvolles Instrument sein, wenn ein Account wiederholt dazu genutzt wird, Personen zu bedrohen, bloßzustellen, mit intimen Bildern unter Druck zu setzen oder gezielt zu diffamieren. Die bloße Löschung einzelner Inhalte reicht in solchen Konstellationen häufig nicht aus. Allerdings muss eine solche Sperrung verhältnismäßig bleiben und darf nicht zu einer automatisierten oder pauschalen Einschränkung zulässiger Kommunikation führen.

Entscheidend wird zudem sein, ob Accountsperren in der Praxis wirksam sind. Wenn Täterinnen und Täter unmittelbar neue Profile anlegen und ihr Verhalten fortsetzen, bleibt die Maßnahme weitgehend wirkungslos. Anbieter müssen deshalb verpflichtet werden, zumutbare technische Möglichkeiten zur Verhinderung solcher Umgehungen auszuschöpfen. Gerade große Plattformen dürfen sich nicht vorschnell darauf zurückziehen können, dass dies technisch oder wirtschaftlich nicht leistbar sei.

Zudem können zivilrechtliche Auskünfte mittelbare Auswirkungen auf Strafverfolgungsbehörden haben. Wenn nach einer zivilgerichtlichen Identifizierung Strafanzeigen, Folgeermittlungen, Akteneinsichten oder weitere Verfahren entstehen, kann auch bei Polizei und Staatsanwaltschaften zusätzlicher Aufwand entstehen. Dieser Aufwand sollte in der Gesetzesfolgenabschätzung nicht unterschätzt werden.

7. Materiellrechtliche Anpassungen im Bereich digitaler Inhalte

Der Entwurf enthält neben den zivilrechtlichen Instrumenten wesentliche Änderungen und Erweiterungen im Strafrecht. Dies betrifft insbesondere sexualisierte Bildinhalte, Deepfakes, manipulierte Inhalte, kinder- und jugendpornografische Inhalte sowie technische Überwachung.

Der BDK begrüßt grundsätzlich, dass der Gesetzgeber auf neue digitale Tatbegehungsformen reagiert. Digitale Gewalt ist für Betroffene nicht weniger real, wenn sie über manipulierte Bilder, synthetische Inhalte oder technische Überwachung begangen wird. Sexualisierte Deepfakes können Menschen in intime oder pornografische Kontexte stellen, die nie stattgefunden haben. Nicht sexualisierte Deepfakes können Personen Aussagen, Handlungen oder Situationen zuschreiben, die geeignet sind, berufliche Existenzen, persönliche Reputation oder politische Glaubwürdigkeit erheblich zu beschädigen. Technische Überwachung durch Tracker, Apps oder andere digitale Mittel kann ein wesentliches Element von Stalking, häuslicher Gewalt und gezielter Einschüchterung sein.

Gerade deshalb ist eine strafrechtliche Nachschärfung in diesen Bereichen grundsätzlich nachvollziehbar und notwendig. Zugleich müssen die Tatbestände so formuliert werden, dass sie bestimmt, trennscharf und praxistauglich bleiben. Die technische Entwicklung generativer KI-Systeme verläuft hochdynamisch. Begriffe wie „wirklichkeitsnah“, „täuschend echt“ oder der „Anschein eines tatsächlichen Geschehens“ können in der Praxis erhebliche Auslegungsfragen aufwerfen. Was heute noch eindeutig als künstlich erkennbar ist, kann morgen bereits realistisch wirken. Umgekehrt darf nicht jede erkennbare digitale Bearbeitung vorschnell in einen strafrechtlichen Kontext gezogen werden.

7.1 § 184b StGB – Kinderpornografische Inhalte

§ 184b StGB stellt die Verbreitung, den Erwerb und den Besitz kinderpornografischer Inhalte unter hohe Strafandrohung. Historisch beruht diese Norm auf der tragenden dogmatischen Annahme, dass entsprechende Inhalte regelmäßig reale sexuelle Missbrauchshandlungen dokumentieren, dass jede Verbreitung die Viktimisierung realer Opfer perpetuiert und dass Nachfrage- und Verbreitungsketten unmittelbar mit realen Missbrauchstaten verbunden sind. Diese Begründung trägt die erhebliche strafrechtliche Eingriffsintensität der Norm.

Der Entwurf berücksichtigt zunehmend auch synthetisch erzeugte oder wirklichkeitsnahe Darstellungen. Damit verschiebt sich die normative Grundlage jedenfalls dort, wo keine konkret dokumentierte Missbrauchshandlung zugrunde liegt. In solchen Konstellationen geht es nicht mehr zwingend um die Verbreitung einer realen Tatdokumentation oder eine unmittelbare Re-Viktimisierung durch das erneute Zugänglichmachen einer tatsächlichen Missbrauchsdarstellung. Die Strafbarkeit stützt sich dann stärker auf abstrakte Gefährdungsannahmen, mögliche Nachfrageeffekte, die Normalisierung missbrauchsbezogener Darstellungen sowie die erhebliche Erschwerung der Abgrenzung zwischen realem und synthetischem Material.

Der BDK weist darauf hin, dass diese Verschiebung eine erhebliche dogmatische Präzisierung erfordert. Dies gilt insbesondere im Hinblick auf die Verhältnismäßigkeit strafrechtlicher Eingriffe, den Bestimmtheitsgrundsatz des Art. 103 Abs. 2 GG sowie die Abgrenzung zwischen realitätsbasierten, manipulierten und vollständig synthetischen Inhalten.

Dabei darf allerdings nicht der Eindruck entstehen, synthetisch erzeugte kinderpornografische Darstellungen seien harmlos. Auch solche Inhalte können reale Kinder als Vorlage nutzen, reale Betroffene erneut schädigen, Täterfantasien bedienen, Nachfrageeffekte verstärken und die Ermittlungsarbeit erheblich erschweren. Gerade deshalb muss der Gesetzgeber die unterschiedliche Unrechtsstruktur sauber herausarbeiten und klar begründen, welches Rechtsgut in welcher Weise betroffen ist und warum die jeweilige Strafandrohung angemessen ist.

Zur Vermeidung missverständlicher Außenwirkung ist klarzustellen: Der BDK plädiert nicht für eine Abschwächung des Schutzes von Kindern und Jugendlichen. Im Gegenteil geht es darum, den Schutz gerade in technisch neuen Erscheinungsformen so auszugestalten, dass er strafrechtlich belastbar, verfassungsrechtlich tragfähig und in der Ermittlungs- und Gerichtspraxis tatsächlich durchsetzbar ist.

7.2 § 184c StGB – Jugendpornografische Inhalte

Für § 184c StGB gelten vergleichbare Erwägungen. Auch hier ist eine zunehmende Konfrontation mit digitalen und KI-generierten Inhalten festzustellen, die Abgrenzungsfragen hinsichtlich jugendtypischer Kommunikation, fiktionaler Darstellungen und strafwürdiger Inhalte verschärfen.

Gerade im Bereich jugendpornografischer Inhalte ist die praktische Abgrenzung besonders sensibel. Strafrechtlicher Schutz von Jugendlichen vor Ausbeutung und sexualisierter Darstellung ist zwingend erforderlich. Gleichzeitig müssen jugendtypische Kommunikationsformen, einvernehmliche Konstellationen im altersnahen Bereich sowie vollständig fiktionale oder synthetische Inhalte dogmatisch sauber von strafwürdigem Verhalten abgegrenzt werden. Andernfalls drohen erhebliche Unsicherheiten in der Anwendungspraxis.

Der BDK regt deshalb an, auch bei § 184c StGB die Abgrenzung zwischen realen, realitätsbasierten, manipulierten und vollständig synthetischen Darstellungen ausdrücklich und praxistauglich zu konturieren.

7.3 § 184k StGB – Digitale und KI-generierte sexuelle Darstellungen

Der neu gefasste beziehungsweise erweiterte § 184k StGB erfasst insbesondere realitätsnah wirkende, jedoch künstlich erzeugte sexuelle Darstellungen, einschließlich sogenannter Deepfake-Inhalte.

Der BDK sieht insbesondere in Tatbestandsmerkmalen wie „wirklichkeitsnah“, „täuschend echt“ sowie „Anschein eines tatsächlichen Geschehens“ erhebliche Auslegungs- und Abgrenzungsprobleme. Diese Begriffe sind technisch dynamisch und verändern sich durch die

Weiterentwicklung generativer KI-Systeme fortlaufend. Was heute noch als manipuliert erkennbar ist, kann morgen kaum noch von realem Bild- oder Videomaterial zu unterscheiden sein.

Dies betrifft insbesondere die Abgrenzung zu künstlerischen, satirischen oder spielerischen Kontexten digitaler Kommunikation. Strafrechtlich relevant muss der gezielte Eingriff in Intimsphäre, sexuelle Selbstbestimmung oder Persönlichkeitsrecht bleiben. Nicht jede digitale Bearbeitung, nicht jede erkennbare Satire und nicht jede fiktive Darstellung darf in denselben strafrechtlichen Bewertungskontext geraten wie eine gezielte sexualisierte Herabwürdigung oder Bloßstellung einer realen Person.

Der BDK regt deshalb an, die strafrechtlichen Tatbestände im weiteren Verfahren besonders sorgfältig auf Bestimmtheit, technische Nachweisbarkeit und Abgrenzbarkeit zu prüfen. Dies betrifft insbesondere die Grenzziehung zwischen realitätsbasierten Manipulationen, vollständig synthetischen Inhalten, satirischen oder künstlerischen Darstellungen und strafwürdigem persönlichkeitsverletzendem Verhalten.

Gleichzeitig ist aus kriminalpolizeilicher Sicht zu berücksichtigen, dass Polizei und Justiz künftig verstärkt klären müssen, ob ein Bild real, manipuliert, realitätsbasiert oder vollständig synthetisch erzeugt wurde. Dafür braucht es forensische Kompetenz, technische Werkzeuge, einheitliche Bewertungsstandards und klare rechtliche Kriterien. Nur dann können die neuen Tatbestände in der Praxis rechtssicher und wirksam angewendet werden.

7.4 § 202e StGB-E – Unbefugte Überwachung mittels Informations- oder Kommunikationstechnik

Der Entwurf sieht mit § 202e StGB-E einen neuen Straftatbestand zur unbefugten Überwachung mittels Informations- oder Kommunikationstechnik vor. Der BDK hält es grundsätzlich für richtig, digitale Überwachungsformen strafrechtlich stärker in den Blick zu nehmen. Ortungsgeräte, Tracking-Apps, manipulierte Geräte oder andere technische Mittel können erhebliche Eingriffe in die persönliche Freiheit und Sicherheit Betroffener darstellen. Sie können insbesondere im Zusammenhang mit Stalking, häuslicher Gewalt, Trennungskonflikten und gezielter Einschüchterung eine erhebliche Rolle spielen.

Gleichwohl sieht der BDK bei der konkreten Fassung des § 202e StGB-E erheblichen Präzisierungsbedarf. Nach Satz 2 des Entwurfs soll Satz 1 nur anzuwenden sein, wenn die Handlung wahrscheinlich dazu führt, dass der betroffenen Person schwerer Schaden zugefügt wird. Diese Formulierung wirft erhebliche Fragen im Hinblick auf das Bestimmtheitsgebot des Art. 103 Abs. 2 GG auf.

Nach der Begründung soll es ausreichen, dass der Schadenseintritt im Einzelfall in Anbetracht der Gesamtumstände der Tat bei einem regelmäßigen Geschehensablauf naheliegt. Sowohl die Wahrscheinlichkeit des Schadenseintritts als auch die Bewertung eines „schweren Schadens“ enthalten erhebliche wertende Elemente. Hinzu kommt, dass die Schwere eines Schadens nicht ohne Weiteres allgemeingültig bestimmt werden kann, weil sie in vielen Konstellationen maßgeblich von der konkreten Situation und der individuellen Opferperspektive abhängt.

Gerade bei digitaler Überwachung können die Folgen für Betroffene sehr unterschiedlich sein. Für eine Person kann eine wiederholte Standortüberwachung bereits eine massive Einschränkung des Sicherheitsgefühls und der Bewegungsfreiheit bedeuten, während dieselbe technische Handlung in einer anderen Konstellation anders zu bewerten sein kann. Diese notwendige Einzelfallbetrachtung darf nicht dazu führen, dass die Strafbarkeit im Kern von schwer vorhersehbaren Wertungen abhängt.

Der BDK regt daher an, § 202e StGB-E tatbestandlich präziser zu fassen. Der Gesetzgeber sollte klarer bestimmen, welche Art von Überwachung, welche Intensität, welche Dauer, welche Wiederholung und welche Schadensqualität für die Strafbarkeit erforderlich sein sollen. Nur so kann gewährleistet werden, dass der Tatbestand wirksam gegen digitale Überwachung eingesetzt werden kann, ohne zugleich erhebliche Unsicherheiten für Strafverfolgung, Gerichte und Normadressaten zu erzeugen.

7.5 Relative Antragsdelikte und öffentliches Interesse an der Strafverfolgung

Der BDK weist ergänzend darauf hin, dass die im Entwurf vorgesehenen oder geänderten Tatbestände, insbesondere § 184k StGB-E, § 201b StGB-E und § 202e StGB-E, als relative Antragsdelikte ausgestaltet werden beziehungsweise in diese Systematik eingebunden sind. Dies ist mit Blick auf Persönlichkeitsrechte und die Dispositionsbefugnis der Betroffenen grundsätzlich nachvollziehbar.

Gleichwohl sollte der Gesetzgeber deutlicher herausarbeiten, in welchen Fallgruppen ein besonderes öffentliches Interesse an der Strafverfolgung regelmäßig naheliegt. Dies betrifft insbesondere massenhafte oder automatisierte Verbreitung, wiederholte Angriffe, organisierte Täterstrukturen, minderjährige Betroffene, sexualisierte Deepfakes, Einschüchterungslagen sowie Fälle, in denen digitale und analoge Gewalt ineinandergreifen. Andernfalls besteht die Gefahr, dass die Strafverfolgung faktisch zu stark von der Belastbarkeit einzelner Betroffener abhängt, obwohl die Tat über den Einzelfall hinaus erhebliche Sicherheits- und Einschüchterungswirkungen entfalten kann.

8. Erreichbarkeit von Plattformen und Zustellungsbevollmächtigte

Der BDK begrüßt, dass der Entwurf die Erreichbarkeit von Plattformen und Diensteanbietern stärker in den Blick nimmt. Gerade bei digitaler Gewalt sind unklare Zustellwege, ausländische Unternehmenssitze und schwer greifbare Verantwortlichkeiten ein erhebliches Vollzugsproblem.

Für Betroffene macht es keinen Unterschied, ob eine Plattform organisatorisch in einem Drittstaat, in einem anderen EU-Mitgliedstaat oder in komplexen Konzernstrukturen organisiert ist. Entscheidend ist, dass sie in Deutschland genutzt wird und dass über sie Rechtsverletzungen begangen werden können. Wer hier erhebliche Reichweite erzielt, muss auch für rechtliche Verfahren verlässlich adressierbar sein.

Der BDK hält deshalb Regelungen für erforderlich, die Gerichten und Betroffenen einen klaren, schnellen und rechtssicheren Zugang zu den jeweiligen Anbietern ermöglichen. Ohne funktionierende Zustellung und verbindliche Kommunikationswege bleiben viele Rechtsansprüche

praktisch schwer durchsetzbar. Die vorgesehene Benennung inländischer Zustellungsbevollmächtigter kann hierzu einen wichtigen Beitrag leisten.

9. Ermittlungspraktische Anforderungen

Der BDK weist darauf hin, dass neue zivilrechtliche Verfahren und neue Straftatbestände nur dann Wirkung entfalten, wenn sie praktisch handhabbar sind. Digitale Gewalt stellt Polizei und Justiz vor erhebliche technische und organisatorische Anforderungen.

Ermittlungen in diesem Bereich betreffen Plattformauskünfte, IP-Zuordnungen, internationale Datenwege, Cloud-Speicher, verschlüsselte Kommunikation, Bild- und Videoforensik, KI-generierte Inhalte und häufig grenzüberschreitende Täterstrukturen. Viele dieser Verfahren sind zeitkritisch. Wenn Daten nicht rechtzeitig gesichert werden, sind sie für die weitere Rechtsdurchsetzung verloren. Die gesetzgeberischen Änderungen müssen deshalb mit einer realistischen Ressourcenplanung verbunden werden. Es braucht spezialisierte digitale Ermittlungsstrukturen, kontinuierliche Fortbildung, moderne Analyse- und Sicherungswerkzeuge, klare Standards für Anbieteranfragen und Datenübermittlungen sowie belastbare internationale Kooperationswege.

Besonders bedeutsam ist die technische Qualität der Auskünfte. IP-Adresse, Portnummer, sekundengenaue Zeitangabe, Zeitzone und Zuordnungslogik müssen so dokumentiert werden, dass sie gerichtsfest verwertbar sind. Unvollständige, uneinheitliche oder technisch unklare Auskünfte führen in der Praxis dazu, dass die Identifizierung trotz rechtlicher Möglichkeit scheitert.

Zugleich darf die Identifizierbarkeit über IP-Daten nicht überschätzt werden. VPN-Dienste, Tor-Nutzung, öffentliche WLANs, Mobilfunk-NAT, Mehrpersonenhaushalte, gemeinsam genutzte Endgeräte oder falsch beziehungsweise unvollständig geführte Nutzungsdaten können dazu führen, dass eine IP-Zuordnung lediglich einen Anschluss oder eine technische Nutzungsspur, nicht aber ohne Weiteres die handelnde Person bezeichnet. Die IP-Adresse ist daher häufig ein wichtiger Ermittlungsansatz, aber kein automatischer Täternachweis.

Wir regen an, diese strukturellen Grenzen ausdrücklich in der Gesetzesbegründung zu benennen. Dies schützt Betroffene vor überzogenen Erwartungen, verhindert Fehlinterpretationen in der Praxis und unterstreicht zugleich den Bedarf an ergänzenden Ermittlungsmaßnahmen, digitalforensischer Auswertung und qualifizierter polizeilicher Bewertung. Weiterhin sollten im weiteren Verfahren nicht nur die rechtlichen Anspruchsgrundlagen, sondern auch die technischen Mindeststandards für Datensicherung und Datenübermittlung stärker in den Blick genommen werden.

10. Evaluation und Nachsteuerung

Aus unserer Sicht ist es notwendig, die tatsächlichen Auswirkungen der Regelungen nach Inkrafttreten sorgfältig zu evaluieren. Dabei sollte die Evaluation nicht auf einzelne zivilrechtliche Verfahrensaspekte beschränkt bleiben. Gerade weil der Entwurf „digitale Gewalt“ und das

Vorhaben zur IP-Adressspeicherung gemeinsam eine neue Architektur digitaler Identifizierung prägen, müssen auch ihre Wechselwirkungen untersucht werden.

Zu prüfen ist insbesondere, wie schnell Daten tatsächlich gesichert werden, wie häufig die Identifizierung von Täterinnen und Tätern gelingt, wie zuverlässig Plattformen und Provider reagieren, wie lange gerichtliche Verfahren dauern, welche Mehrbelastung bei Polizei, Staatsanwaltschaften und Gerichten entsteht und ob es zu unbeabsichtigten Verschiebungen zwischen zivilrechtlicher und strafprozessualer Rechtsdurchsetzung kommt.

Eine solche Evaluation sollte ausdrücklich Polizei, Staatsanwaltschaften, Gerichte, Anbieterpraxis und Opferperspektive einbeziehen. Nur so lässt sich feststellen, ob die Regelungen den Schutz vor digitaler Gewalt tatsächlich verbessern oder ob gesetzgeberischer Nachsteuerungsbedarf besteht.

11. Forderungen des BDK

- Die beiden parallel geführten Gesetzgebungsvorhaben sollten ausdrücklich als zusammenhängendes System digitaler Rechtsdurchsetzung behandelt und die Schnittstellen zwischen zivilrechtlicher Auskunft, strafprozessualem Zugriff und späterer Datenverwertung klarer geregelt werden.

- Erforderlich ist aus unserer Sicht insbesondere eine gesetzgeberische Klarstellung zur Verwertbarkeit zivilgerichtlich erlangter Provider-Daten im Strafverfahren, einschließlich Zweckbindung, Dokumentation, Datenintegrität und Rechtsschutz. Ebenso sollten die technischen Mindeststandards für Datensicherung und Datenübermittlung, insbesondere IP-Adresse, Portnummer, Zeitstempel, Zeitzone und Zuordnungslogik, verbindlicher gefasst werden.

- Der Gesetzgeber sollte die strukturellen Grenzen der IP-basierten Identifizierung ausdrücklich benennen und durch eine realistische Darstellung der Beweisbedeutung solcher Daten flankieren. IP-Zuordnungen sind regelmäßig wichtige Ermittlungsansätze, ersetzen aber nicht die kriminalpolizeiliche Bewertung und weitere Beweiserhebung.

- Für die relativen Antragsdelikte sollte die Gesetzesbegründung klarer herausarbeiten, wann ein besonderes öffentliches Interesse an der Strafverfolgung regelmäßig anzunehmen ist. Dies gilt insbesondere bei wiederholten, massenhaften, sexualisierten, gegen Minderjährige gerichteten oder einschüchternden digitalen Angriffen.

- Schließlich fordert der BDK eine auskömmliche personelle, technische und organisatorische Ausstattung von Polizei, Staatsanwaltschaften und Gerichten. Neue zivilrechtliche Instrumente und neue Straftatbestände werden nur dann Wirkung entfalten, wenn die zuständigen Stellen digitale Spuren schnell sichern, technisch bewerten, rechtlich einordnen und gerichtsfest verwerten können.

12. Gesamtbewertung

Der Bund Deutscher Kriminalbeamter unterstützt die Zielrichtung des Entwurfs zur Stärkung des zivilrechtlichen und strafrechtlichen Schutzes vor digitaler Gewalt. Der Entwurf erkennt an, dass

digitale Gewalt reale Folgen hat und dass Betroffene wirksame Wege benötigen, um Täterinnen und Täter zu identifizieren, Rechtsverletzungen zu unterbinden und Ansprüche durchzusetzen.

Zugleich weisen wir darauf hin, dass der Entwurf im Zusammenhang mit dem Gesetzgebungsvorhaben zur Speicherung und Nutzung von IP-Adressdaten betrachtet werden muss.

Beide Vorhaben bilden gemeinsam eine neue Architektur digitaler Identifizierung. Diese Architektur darf nicht zu Wertungsbrüchen führen. Insbesondere muss der Gesetzgeber nachvollziehbar begründen, wie sich die zivilrechtliche Identifizierung über IP-Daten zu den strafprozessualen Zugriffsschwellen verhält.

Der BDK sieht keinen zwingenden Grund, das zivilrechtliche Auskunftsverfahren in Frage zu stellen. Er sieht aber erheblichen Klärungsbedarf bei der Abstimmung mit den strafprozessualen Befugnissen, bei der technischen Ausgestaltung der Datensicherung, bei den Anforderungen an Anbieter und bei den praktischen Folgen für Polizei, Staatsanwaltschaften und Gerichte.

13. Fazit

Digitale Gewalt ist eine reale Bedrohung für persönliche Freiheit, Intimsphäre, gesellschaftliche Teilhabe und Vertrauen in den Rechtsstaat. Der Staat muss auch dort handlungsfähig sein, wo Straftaten über Accounts, Plattformen, Messenger, Cloud-Dienste, IP-Adressen und technische Überwachungsmittel begangen werden.

Der Entwurf „digitale Gewalt“ ist hierfür ein wichtiger Schritt. Er stärkt Betroffene, verbessert Auskunfts- und Sicherungsmöglichkeiten und schafft klarere strafrechtliche Antworten auf Deepfakes, bildbasierte sexualisierte Gewalt und technische Überwachung. Damit diese Regelungen wirken, müssen sie jedoch in eine kohärente Gesamtstruktur eingebettet werden.

Der BDK spricht sich deshalb für die Weiterführung des Gesetzgebungsvorhabens aus. Zugleich regt er an, beide parallelen Regelungskomplexe gemeinsam zu betrachten, Wertungsinkongruenzen zwischen zivilrechtlicher und strafprozessualer Identifizierung zu vermeiden, die strafrechtlichen Tatbestände technisch und dogmatisch präzise auszugestalten und Polizei sowie Justiz so auszustatten, dass der Schutz vor digitaler Gewalt nicht nur gesetzlich formuliert, sondern im Alltag tatsächlich durchgesetzt werden kann.

Mit freundlichen Grüßen

Dirk Peglow
Bundesvorsitzender