HANDLUNGSFELD DIGITALER RAUM

Kleine Beträge, gravierende Folgen

Finanztransaktionen zur sexuellen Ausbeutung von Minderjährigen im digitalen Raum

ECPAT POLICY BRIEF

Soziale Plattformen, Messenger-Dienste, Online-Games und weitere digitale Anwendungen gehören mittlerweile zum Lebensalltag dazu — auch für Kinder und Jugendliche. Dies stellt unsere Gesellschaft vor eine doppelte Herausforderung: digitale Teilhabe zu fördern und Kinder gleichzeitig vor den Risiken zu schützen, die dieser Raum birgt. Eine der gravierendsten Gefahren ist die sexualisierte Gewalt und Ausbeutung im digitalen Raum. Weltweit sind aktuell pro Jahr über 300 Millionen Kinder und Jugendliche davon betroffen.[1]

Monetarisierung sexualisierter Gewalt und ihre Folgen

Digitalisierung und neue Technologien haben tiefgreifend verändert, wie sexualisierte Gewalt gegen Kinder und Jugendliche organisiert und monetarisiert wird. Finanztransaktionen sind integrale Bestandteile weit verbreiteter Ausbeutungsformen:

→ Bei der **sexuellen Ausbeutung per Livestreaming** werden Zahlungen unmittelbar an einzelne Interaktionsereignisse gekoppelt. Die se-xualisierte Gewalt wird live an Täter(*innen)[2] übertragen, die vor und während der Tat Anweisungen geben — per Chat oder Mikrofon. In der Regel sind mindestens zwei Tatpersonen beteiligt: Die nachfragende Person, die überwiegend aus westlichen Ländern einschließlich EU-Staaten stammt und einer ermöglichenden Person, die sich gemeinsam mit den betroffenen Kindern und Jugendlichen vor Ort befindet — oft in Ländern des Globalen Südens. Allein auf den Philippinen sind knapp eine halbe Million Kinder und Jugendliche von dieser Ausbeutungsform betroffen. Viele Betroffene berichten, dass die erlebte Gewalt ohne die Zahlungstransaktion nicht stattgefunden hätte.[3] Der aktuelle Europol Bericht weist darauf hin, dass es auch betroffene Kinder und Jugendliche in der EU gibt, die von Täter(*innen) aus der EU per Livestreaming ausgebeutet werden.[4]

→ Bei der **finanziell motivierten sexuellen Erpressung** (FMSE) werden Kinder und Jugendliche unter Druck gesetzt, Zahlungen zu leisten — unter Androhung der Veröffentlichung intimer Bilder oder Videos, die entweder in einem Vertrauensverhältnis geteilt, durch Manipulation oder Druck erlangt oder mithilfe von KI künstlich erzeugt wurden (sog. Deepnudes). 2025 wurden im Schnitt 137 Fälle pro Tag allein beim National Center for Missing and Exploited Children gemeldet — ein Anstieg von 37 % gegenüber dem Vorjahr.[5]

1 Childlight (2024). Into the Light Index on child sexual exploitation and abuse globally: 2024 report. Edinburgh: Childlight — Global Child Safety Institute.

2 In unseren Texten verwenden wir die Schreibweise ›Täter(*innen)‹. Das liegt daran, dass die Mehrheit der Täter(*innen) männlich ist. Trotzdem gilt: Sexualisierte Gewalt kann auch von Frauen oder Menschen anderen Geschlechts ausgehen.

3 International Justice Mission and University of Nottingham Rights Lab (2023). Scale of Harm Research Method, Findings, and Recommendations: Estimating the Prevalence of Trafficking to Produce Child Sexual Exploitation Material in the Philippines. International Justice Mission.

4 Europol (2026) The evolving threat landscape. How encryption, proxies and AI are expanding cybercrime — Internet Organised Crime Threat Assessment (IOCTA) 2026, Publications Office of the European Union, Luxembourg.

5 National Center for Missing & Exploited Children (2026). 2025 CyberTipline Report.

- Bei **›Taschengeld-Treffen‹** werden Kinder und Jugendliche zu sexuellen Handlungen gegen finanzielle oder materielle Gegenleistungen verleitet. Als Plattformen dienen nicht nur einschlägige Erotik-Portale, sondern auch unauffällige Kleinanzeigen-Portale.[6] 2024 wurden in Deutschland 30 solcher Fälle polizeilich registriert[7], Fachberatungsstellen gehen jedoch von einer erheblichen Dunkelziffer aus.
- Auch bei der Herstellung und Verbreitung von **Darstellungen sexualisierter Gewalt gegen Kinder und Jugendliche** können monetäre Gegenleistungen eine Rolle spielen. Anders als bei den vorgenannten Ausbeutungsformen, sind finanzielle Transaktionen hier kein konstituierendes Merkmal des Phänomens, da es auch zum nicht-kommerziellen Austausch von Darstellungen kommen kann.

Die Folgen für Betroffene sind gravierend und vielschichtig. Neben unmittelbaren Traumatisierungen berichten viele Kinder und Jugendliche von anhaltendem psychischem Druck, sozialer Isolation und dem Gefühl, keine Kontrolle über das eigene Leben zu haben. Der zusätzliche finanzielle Druck verstärkt diesen Kontrollverlust noch mehr. Die psychischen Folgen können schwerwiegend sein und unter anderem zu Suchtproblemen, selbstverletzendem Verhalten oder Suizid führen. Das National Center for Missing and Exploited Children dokumentierte 2025 knapp 30 Suizide betroffener Minderjähriger im Zusammenhang mit finanziell motivierter sexueller Erpressung — eine Zahl, die das tödliche Ausmaß dieser Gewaltform in aller Deutlichkeit belegt.[8]

6 ECPAT Deutschland e. V. (2025). Taschengeld-Treffen: Sexuelle Ausbeutung von Minderjährigen und die Rolle von Online-Anzeigenportalen.

7 Bundeskriminalamt (2025). 2024 Bundeslagebild Menschenhandel und Ausbeutung.

8 National Center for Missing & Exploited Children (2026). 2025 CyberTipline Report.

Rechte für Kinder — Regeln für Digitales

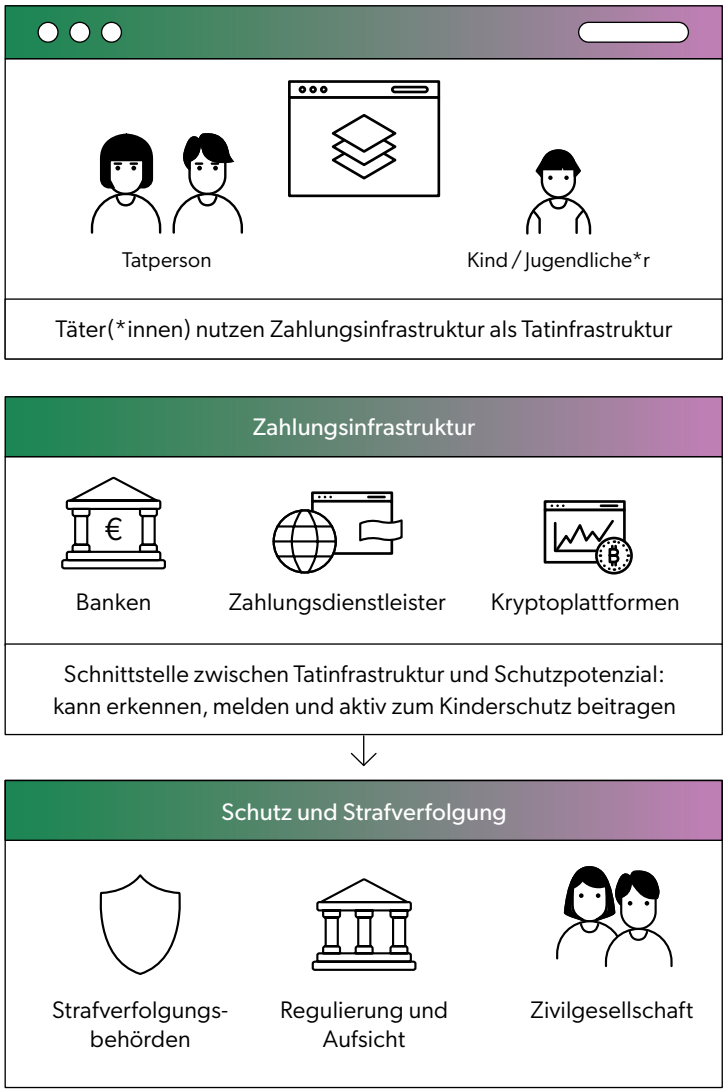
Digitale sexualisierte Gewalt gegen Kinder und Jugendliche ist eine schwerwiegende Verletzung grundlegender Kinderrechte. Die UN-Kinderrechtskonvention (KRK) verpflichtet Vertragsstaaten, Kinder vor allen Formen sexueller Ausbeutung und sexualisierter Gewalt zu schützen (Art. 34 KRK). Die Allgemeine Bemerkung Nr. 25 bestätigt die uneingeschränkte Gültigkeit der KRK im digitalen Raum. Das Fakultativprotokoll zur KRK über »den Verkauf von Kindern, die Kinderprostitution und die Kinderpornographie« konkretisiert diese Pflichten und fordert ausdrücklich Maßnahmen gegen finanzielle Transaktionen, die mit der Ausbeutung von Kindern verbunden sind. Auch die UN-Leitprinzipien für Wirtschaft und Menschenrechte (UNGP) sind eindeutig: Unternehmen tragen Verantwortung dafür, dass ihre Infrastrukturen, Produkte und Dienstleistungen keine Menschenrechtsverletzungen ermöglichen oder begünstigen.

Für Finanzinstitutionen und Plattformunternehmen bedeutet das, nicht zum strukturellen Ermöglicher von Ausbeutung zu werden und aktiv zur Stärkung von Schutzmechanismen beizutragen. Dieser Perspektivwechsel — vom Finanzsektor als passivem Ermöglichungsraum hin zu einem aktiven Schutzakteur — ist der Ausgangspunkt dieses Policy Briefs. Denn während Täter(*innen) die Infrastruktur

von Zahlungsdienstleistern für diese Formen der Ausbeutung nutzen, bieten genau diese Transaktionen gleichzeitig konkrete Ansatzpunkte für Prävention, Aufdeckung und Strafverfolgung.

Die Voraussetzungen für mehr Prävention und bessere Strafverfolgung sind vorhanden: Technische Systeme, regulatorische Rahmenwerke und institutionelle Akteur*innen existieren — zum Beispiel im Bereich der Geldwäschevermeidung und der Terrorismusprävention. Sie können und müssen weiterentwickelt und konsequenter auf den Schutz von Kindern und Jugendlichen ausgerichtet werden.

Tatgeschehen auf digitalen Plattformen



Dieses Policy Brief basiert auf der Studie ›Kleine Beträge, gravierende Folgen: Finanztransaktionen zur sexuellen Ausbeutung von Minderjährigen im digitalen Raum‹ von Dirk Findeisen, die von ECPAT Deutschland e.V. beauftragt wurde. Sie richtet sich an Entscheidungsträger*innen aus Politik, Finanzsektor und Plattformwirtschaft und zeigt auf, wo konkreter Handlungsbedarf besteht.

Zentrale Erkenntnisse

Digitale sexualisierte Gewalt gegen Kinder und Jugendliche findet zunehmend in wirtschaftlich organisierten, technisch vermittelten Strukturen statt. Die finanzielle Dimension dieser Gewalt ist dabei keine Randerscheinung: Sie ist in vielen Ausbeutungsformen mittlerweile strukturell eingebettet, folgt erkennbaren Mustern und bietet damit konkrete Ansatzpunkte für Schutz, Aufdeckung und Strafverfolgung.

Die Studie identifiziert charakteristische Transaktionsmuster. Dazu zählen Mikrotransaktionen, sequenzielle Zahlungsfolgen und plattformübergreifende oder hybride Zahlungsstrukturen. Im Kontext der sexualisierten Gewalt und Ausbeutung von Kindern und Jugendlichen treten diese etwa bei wiederkehrenden Zahlungen für den Zugang zu exklusiven Inhalten oder bei schrittweise eskalierenden Zahlungsaufforderungen gegenüber Betroffenen auf. Relevante Muster erschließen sich dabei häufig erst in der Gesamtschau — nicht auf Ebene einzelner Transaktionen. Klassische Einzeltransaktionsanalysen, wie sie bisher im Bankenwesen vorherrschen, greifen hier strukturell zu kurz.

Im Rahmen der Studie bestätigten Interviewpartner*innen diese Muster: Bei sexueller Ausbeutung via Livestreaming etwa sind die Transaktionen unmittelbar an einzelne Interaktionsereignisse gekoppelt. Es können aber auch Zahlungsserien entstehen — etwa im Rahmen von finanziell motivierter sexueller Erpressung, bei der Kinder und Jugendliche zur Zahlung vieler kleiner Beträge gedrängt werden.

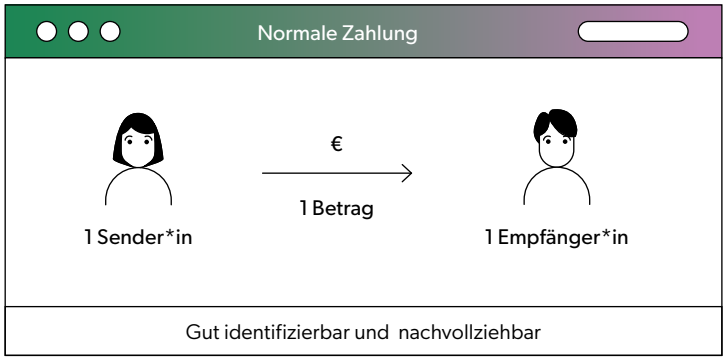
Ein weiterer zentraler Befund betrifft intermediäre Rollen in Transaktionsnetzwerken. Aus internationalen Analysen sind solche Rollen bekannt — etwa bei der Vermittlung zwischen Täter(*innen) und Betroffenen, bei der Distribution von Darstellungen sexualisierter Gewalt innerhalb geschlossener Netzwerke, z. B. im Darknet oder bei der Koordination von Livestreaming-Ausbeutung in verschlüsselten Chat-Gruppen. Die Verknüpfung dieser Netzwerkrollen mit finanziellen Transaktionsströmen ist analytisch besonders wertvoll, aber auch herausfordernd: Zahlungsbeziehungen können Hinweise auf Strukturen und Hierarchien innerhalb eines Netzwerks liefern, die aus Kommunikationsdaten allein nicht sichtbar wären. Für Strafverfolgung und Prävention eröffnet das neue Ermittlungsansätze — und damit Chancen, Kinder und Jugendliche besser zu schützen.

Ein strukturelles Kernproblem bleibt die Fragmentierung des Lagebilds: Kein Akteur verfügt allein über vollständige Informationen. Online-Plattformen sehen Interaktions- und Kommunikationsdaten, während bei Finanzinstitutionen einzelne Transaktionsdaten vorliegen. Im Rahmen von Ermittlungsverfahren muss beides zusammengeführt werden, um Täter(*innen) zur Verantwortung zu ziehen und Betroffene zu schützen.

Bestehende AML / CFT-Systeme[9] stoßen an strukturelle Grenzen, wenn Transaktionen fragmentiert sind, Kontextinformationen fehlen und Zahlungsstrukturen systemübergreifend verteilt sind. Gleichzeitig zeigt die Studie erhebliches, bislang ungenutztes Potenzial — insbesondere durch dynamische Kundenrisikoklassifizierung und die Integration deliktspezifischer Risikoindikatoren. Voraussetzung dafür ist, dass digitale sexualisierte Gewalt und Ausbeutung von Kindern und Jugendlichen als eigenständiger Deliktbereich in Risikomodellen verankert wird, sowohl bei privatwirtschaftlichen Zahlungsdienstleistern als auch im Rahmen von Strafermittlungen. Die Subsummierung unter andere Finanzdelikte ist wenig hilfreich, um Aufdeckungschancen systematisch zu erhöhen.

9 AML = Anti-Money Laundering (Anti-Geldwäsche); CFT = Countering the Financing of Terrorism (Bekämpfung von Terrorismus-Finanzierung)

Auch Plattformarchitekturen sind hochgradig relevant: Sie schaffen oder verschließen strukturelle Möglichkeiten für Ausbeutung und deren Verschleierung. Monetarisierungsfunktionen können Interaktionsanreize für Täter(*innen) schaffen. Wenn gleichzeitig Erkennungs- und Schutzmechanismen fehlen, werden Unternehmen zum Ermöglicher von sexualisierter Gewalt gegen Kinder und Jugendliche. Durch die Anwendung umfassenderer Analysemöglichkeiten sollten Unternehmen ihrer kinderrechtlichen Verantwortung gerecht werden. Im Lichte der gravierenden Zunahme von digitaler kommerzieller Ausbeutung und den massiven Folgen für Betroffene, sollten höhere Schutzstandards auch regulatorisch verankert werden.

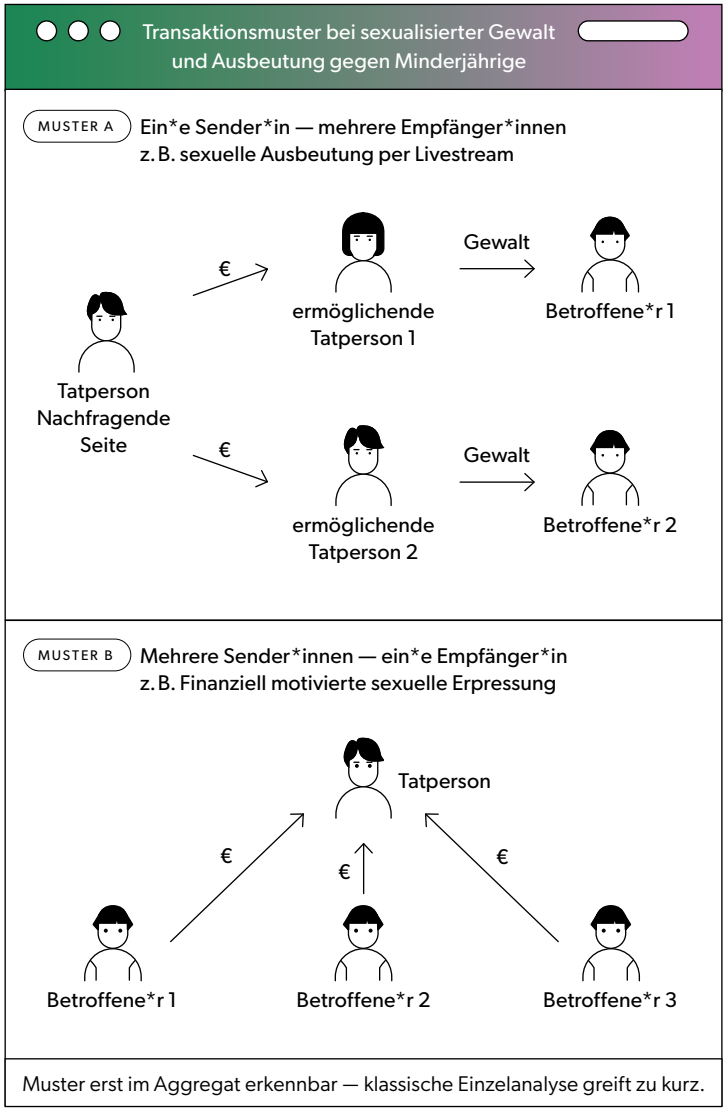


✓ Einmaliger, klarer Betrag

✓ Empfänger*in klar identifizierbar

✓ Nachvollziehbarer Zweck

✓ Ein regulärer Kanal



Gemeinsame Merkmale beider Muster

⚠ Fragmentierte Mikrozahlungen

⚠ Sequenziell und wiederkehrend

⚠ Mehrere Kanäle und Systeme

⚠ Zweck verschleiert oder uneindeutig

Handlungsempfehlungen

REGULATORISCHE UND STAATLICHE AKTEUR*INNEN

Rechtssicherheit für proaktiv handelnde Finanzdienstleister schaffen: Finanzinstitutionen, die verdächtige Transaktionen im Zusammenhang mit digitaler sexualisierter Gewalt gegen Kinder melden, verzögern oder sperren, müssen wirksam vor zivilrechtlichen Schadensersatzforderungen durch betroffene Kund*innen geschützt werden. Gesetzliche Haftungsfreistellungen — vergleichbar bestehenden Safe-Harbor-Regelungen im AML-Kontext — sind eine notwendige Voraussetzung dafür, dass Finanzdienstleister ihrer Schutzverantwortung ohne rechtliches Risiko nachkommen können.

Finanzmarkt- und Plattformregulierung verzahnen: Während Finanzinstitutionen bereits umfassend in AML / CFT-Regime eingebunden sind, fehlen vergleichbare, kinderrechtlich fundierte Anforderungen an die monetären Interaktionsstrukturen digitaler Plattformen. Eine integrierte Regulierungsperspektive, die beide Bereiche verbindet, ist dringend erforderlich.

Monetarisierungsfunktionen als Tatmittel im digitalen Kinderschutzrecht adressieren: Der Digital Services Act und die EU-Leitlinien zum Schutz Minderjähriger betrachten monetäre Aspekte bislang vor allem verbraucherschützend — etwa mit Blick auf manipulative Kaufanreize oder Lootboxen. Die Rolle von Zahlungs-, Gifting- und Peer-to-Peer-Funktionen als Infrastruktur für sexualisierte Gewalt bleibt dabei unberücksichtigt. Diese Lücke sollte durch verbindliche child-rights-by-design-Anforderungen an monetäre Interaktionsfunktionen und deren Einbeziehung in die Risikobewertungen sehr großer Plattformen geschlossen werden.

Rechtssichere Schnittstellen für den Datenaustausch schaffen: Regulatorische Rahmenwerke sollten die Verknüpfung der komplementären Datenperspektiven von Finanzinstitutionen, Plattformen und staatlichen Stellen gezielt ermöglichen — durch definierte Schnittstellen, rechtlich abgesicherte Austauschformate und Kooperationsplattformen. Auch Public-Private-Partnerships sollten gefördert werden, Initiativen wie das Lantern-Projekt der Tech Coalition könnten bspw. systematisch an europäische Rahmenbedingungen angepasst werden.

FINANZSEKTOR UND ZAHLUNGSDIENSTLEISTER

Sequenzbasierte Analyseverfahren einführen: Bestehende Monitoring-Systeme sollten um verhaltens- und sequenzbasierte Analysemodelle ergänzt werden. Fragmentierte Mikrotransaktionen und wiederkehrende Zahlungsfolgen entfalten ihre Aussagekraft erst im Aggregat — klassische Einzeltransaktionsanalysen erfassen diese Muster unzureichend.

Dynamische Kundenrisikoklassifizierung stärken: Kundenrisikoprofile sollten kontinuierlich aktualisiert und um deliktspezifische Risikoindikatoren aus dem Bereich digitaler sexualisierter Gewalt ergänzt werden. In eigenen Risikoanalysen sollte digitale sexualisierte Gewalt und Ausbeutung von Kindern und Jugendlichen als eigenständiger Deliktbereich verankert werden — nicht lediglich als Unterfall allgemeiner Finanzkriminalität.

Kooperation im Analyseökosystem ausbauen: Finanzinstitutionen müssen ihre Rolle als Teil eines übergreifenden Analyseverbunds verstehen und die strukturierte Zusammenarbeit mit Zahlungsdienstleistern, Analyseunternehmen und staatlichen Stellen intensivieren, um bestehende Informationslücken zu schließen.

DIGITALE PLATTFORMEN UND TECHNOLOGIEUNTERNEHMEN

Child-rights-by-design und Safety-by-design als Entwicklungsprinzip verankern: Plattformfunktionen und Monetarisierungsmodelle müssen konsequent daraufhin geprüft werden, ob sie unbeabsichtigte Anreize oder strukturelle Möglichkeiten für Ausbeutungs- und Gewalthandlungen schaffen. Kinderschutz muss dabei von Beginn an als Designanforderung — nicht als nachträgliche Korrekturmaßnahme — verstanden werden.

Monetäre Dimensionen in Sicherheitsmechanismen integrieren: Interaktions- und Zahlungsprozesse sind auch dann funktional verbunden, wenn die Zahlungsabwicklung außerhalb der Plattform erfolgt. Kontextinformationen aus Interaktionen sollten systematisch in Moderations- und Erkennungsmechanismen einfließen, um potenzielle Risikostrukturen frühzeitig zu identifizieren.

Netzwerk- und Interaktionsanalysen ausbauen: Relevante Risikomuster entstehen häufig erst im Kontext von Interaktionsnetzwerken und wiederkehrenden Verhaltensmustern, nicht auf Ebene einzelner Inhalte oder Nutzenden. Plattformen sollten ihre Analysefähigkeiten entsprechend weiterentwickeln und durch strukturierte, aggregierte Berichte zur sektorübergreifenden Wissensbildung beitragen.

SEKTORÜBERGREIFENDE KOOPERATION ALS SCHLÜSSELAUFGABE

Die beschriebenen Herausforderungen lassen sich durch keine Institution allein bewältigen. Eine wirksame Analyse und Prävention erfordert die systematische Verknüpfung komplementärer Datenperspektiven — unter strikter Wahrung datenschutz- und grundrechtlicher Anforderungen. Drei Handlungsachsen sind dabei zentral:

Kooperationsstrukturen institutionalisieren: Bestehende Kooperationsformate zwischen Finanzsektor, Plattformen und staatlichen Stellen sind häufig noch fragmentiert und projektbezogen. Sie sollten zu langfristig angelegten, national und international abgestimmten Strukturen weiterentwickelt werden.

Gemeinsame Analysesprache und Risikoindikatorik entwickeln: Unterschiedliche Akteur*innen verfügen über verschiedene Bewertungslogiken. Gemeinsame Trainingsformate, abgestimmte Indikatorsysteme und interdisziplinäre Analyseansätze sind Grundvoraussetzungen für wirksame Kooperation und sektorübergreifende Erkenntnisgewinnung.

Regulierung adaptiv gestalten: Digitale Plattformen, Zahlungsinfrastrukturen und Risikodynamiken entwickeln sich mit hoher Geschwindigkeit. Governance-Modelle müssen auf kontinuierlicher Beobachtung und Anpassung basieren, um strukturellen Veränderungen wirksam begegnen zu können.

Dieses Policy Brief basiert auf der Studie ›Kleine Beträge, gravierende Folgen: Finanztransaktionen zur sexuellen Ausbeutung von Minderjährigen im digitalen Raum‹ von Dirk Findeisen, die von ECPAT Deutschland e. V. beauftragt wurde. Die Studie kombiniert eine umfassende internationale Literaturrecherche mit qualitativen Interviews mit Akteur*innen aus Strafverfolgungsbehörden, Finanzdienstleistung und Zivilgesellschaft. Sie richtet sich an Entscheidungsträger*innen aus Politik, Finanzsektor und Plattformwirtschaft und zeigt auf, wo konkreter Handlungsbedarf besteht.

REDAKTION

Lea Peters (Text)
Antje Monshausen (V. i. S. d. P.)

GESTALTUNG

www.studio-nea.de

HERAUSGEBERIN

ECPAT Deutschland e. V.
Alfred-Döblin-Platz 1
D-79100 Freiburg
+49 (0)761 / 887 926 30
www.ecpat.de

© ECPAT Deutschland e. V.
Juli 2026
Alle Rechte vorbehalten.

NEWSLETTER

www.ecpat.de/newsletter

@ecpatgermany

ECPAT Germany