DIGITAL SPACE

Small Amounts, Grave Consequences

Financial transactions relating to the sexual exploitation of minors in the digital sphere

ECPAT POLICY BRIEF

Social platforms, messenger services, online games and other digital applications are now part of everyday life — for children and youth as well. This presents our society with a dual challenge: promoting digital participation and empowerment while simultaneously protecting children from the risks this space entails. One of the most serious dangers is sexualised violence and exploitation in the digital sphere. Worldwide, more than 300 million children (any person under the age of 18) are currently affected each year.[1]

Monetisation of Sexualised Violence and Its Consequences

Digitalisation and new technologies have profoundly changed how sexualised violence against children is organised and monetised. Financial transactions are integral components of widespread forms of exploitation:

- **Commercial sexual exploitation via livestreaming:** payments are directly linked to individual interaction events. The sexualised violence is streamed live to perpetrators who give instructions before and during the act — via chat or microphone. At least two perpetrators are typically involved: the person demanding the act, who predominantly originates from Western countries including EU member states, and an enabling person who is physically present with the children — often in countries of the Global South. In the Philippines alone, nearly half a million children are affected by this form of exploitation. Many survivors report that the violence they experienced would not have occurred without the payment transaction.[2] The latest Europol report notes that children within the EU are also being exploited via livestreaming by perpetrators based in the EU.[3]
- **Financially motivated sexual extortion (FMSE):** children are pressured into making payments — on the basis of intimate images or videos that were either shared in a relationship of trust, obtained through manipulation or coercion, or artificially generated using AI (so-called deepnudes). In 2025, an average of 137 cases per day were reported to the National Center for Missing and Exploited Children alone — an increase of 37% compared to the previous year.[4]
- **›Pocket money dates‹ (›Taschengeld-Treffen‹):** children are induced to engage in sexual acts in exchange for financial or material compensation. The platforms used are not only dedicated erotic portals, but also inconspicuous classified advertisement portals.[5] In 2024, 30 such cases were registered by

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

2 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.

3 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.

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

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

police in Germany,[6] though specialist counselling centres believe the actual number to be significantly higher.

→ **Production and distribution of child sexual abuse material (CSAM):** monetary payments can also play a role in the production and distribution of material depicting sexualised violence against children. Unlike the forms of exploitation listed above, financial transactions are not a constitutive feature here, as non-commercial exchange of such material also occurs.

The consequences for those affected are serious and multifaceted. In addition to immediate traumatisation, many children report sustained psychological pressure, social isolation, and a sense of having lost control over their own lives. The financial dimension amplifies this loss of control and increases the pressure on children further. The psychological consequences can be severe and may include addiction problems, self-harming behaviour or suicide. The National Center for Missing and Exploited Children documented nearly 30 suicides of affected minors in connection with financially motivated sexual extortion in 2025 — a figure that illustrates the lethal dimension of this form of violence with devastating clarity. [7]

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

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

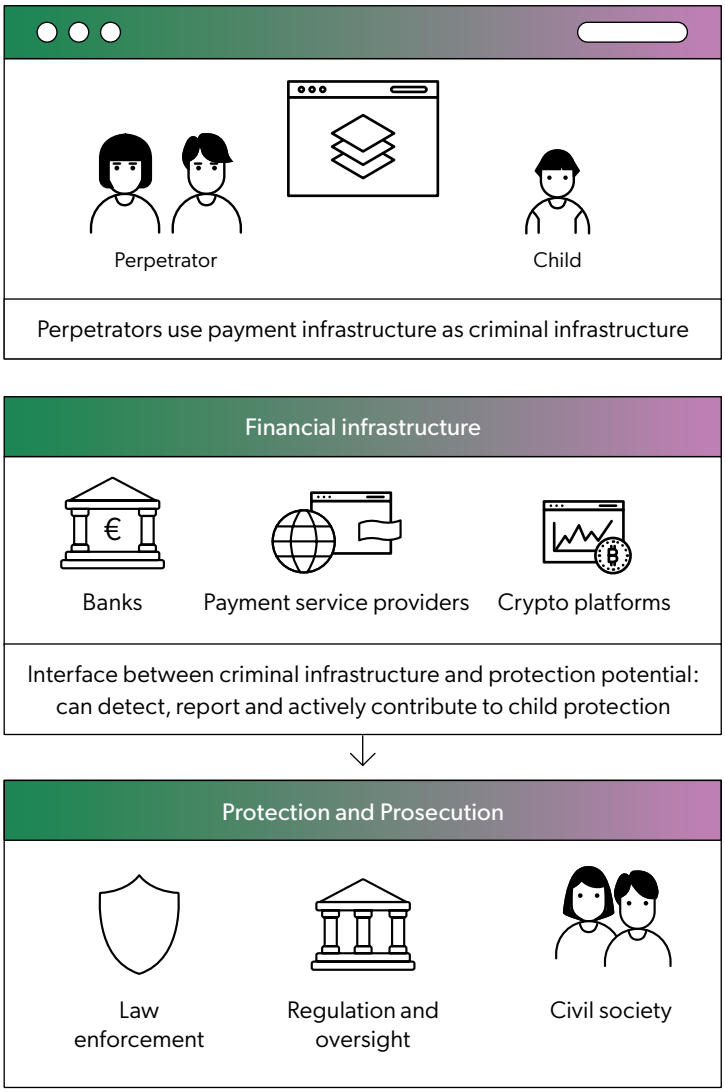
Rights for Children — Rules in the Digital Space

Digital sexualised violence against children constitutes a serious violation of fundamental children's rights. The UN Convention on the Rights of the Child (CRC) obliges State Parties to protect children from all forms of sexual exploitation and sexualised violence (Art. 34 CRC). General Comment No. 25 confirms the full applicability of the CRC in the digital space. The Optional Protocol to the CRC on the ›sale of children, child prostitution and child pornography‹ further specifies these obligations and explicitly calls for measures against financial transactions linked to the exploitation of children. The UN Guiding Principles on Business and Human Rights (UNGPs) are equally clear: companies bear responsibility for ensuring that their infrastructure, products and services do not enable or facilitate human rights violations.

For financial institutions and platform companies, this means not becoming structural enablers of exploitation — and actively contributing to the strengthening of protective mechanisms. This shift in perspective — from the financial sector as a passive enabling space to an active protection actor — is the starting point of this Policy Brief. While perpetrators use the infrastructure of payment service providers for these forms of exploitation, these very transactions simultaneously offer concrete entry points for prevention, detection and prosecution.

The prerequisites for greater prevention and improved prosecution already exist: technical systems, regulatory frameworks and institutional actors are in place — for example in the fields of anti-money laundering and counter-terrorism financing. These can and must be further developed and more consistently aligned with the protection of children.

Criminal Act in digital platforms



This Policy Brief is based on the study ›Kleine Beträge, gravierende Folgen: Finanztransaktionen zur sexuellen Ausbeutung von Minderjährigen im digitalen Raum‹ [›Small Amounts, Grave Consequences: Financial Transactions for the Sexual Exploitation of Minors in the Digital Space‹] by Dirk Findeisen, commissioned by ECPAT Germany. It is aimed at decision-makers from politics, the financial sector and the platform economy, and identifies where concrete action is required.

Key Findings

Digital sexualised violence against children is increasingly taking place within economically organised, technologically mediated structures. The financial dimension of this violence is not a marginal phenomenon: in many forms of exploitation it is now structurally embedded, follows recognisable patterns, and thus offers concrete entry points for protection, detection and prosecution.

The study identifies characteristic transaction patterns, including micro-transactions, sequential payment sequences and cross-platform or hybrid payment structures. In the context of sexualised violence and exploitation of children, these appear for example in recurring payments for access to exclusive content or in gradually escalating payment demands directed at those affected. Relevant patterns often only become apparent when viewed together, not at the level of individual transactions. Classical single-transaction analyses, as currently predominant in the banking sector, are structurally insufficient to capture these patterns.

Interview partners confirmed these patterns in the course of the study: in commercial livestream exploitation, for instance, transactions are directly linked to individual interaction events. However, payment series may also emerge — for example in the context of financially motivated sexual extortion, where children are pressured into making many smaller payments.

A further key finding concerns intermediary roles within transaction networks. Such roles are known from international analyses — for instance in the mediation between perpetrators and victims, in the distribution of material depicting sexualised violence within closed networks (e. g. on the darknet), or in the coordination of livestreaming exploitation in encrypted chat groups. Linking these network roles to financial transaction flows is analytically particularly valuable but also challenging: payment relationships can provide indications of structures and hierarchies within a network that would not be visible from communication data alone. For prosecution and prevention, this opens new investigative approaches — and thus opportunities to better protect children.

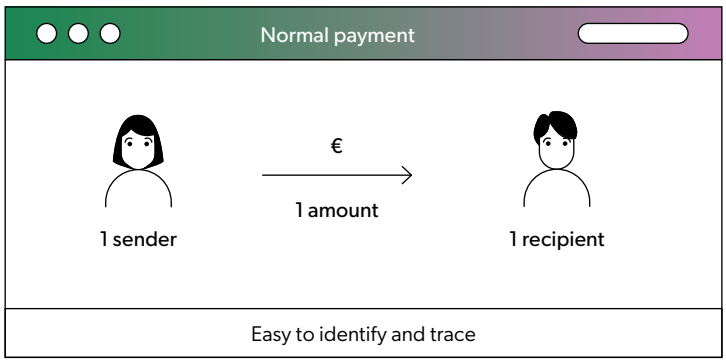
A structural core problem remains the fragmentation of situational awareness: no single actor possesses complete information. Online platforms see interaction and communication data, while financial institutions hold individual transaction data. In the context of investigations, both must be brought together to hold perpetrators accountable and protect those affected.

Existing AML/CFT systems[8] reach structural limits when transactions are fragmented, contextual information is lacking and payment structures are distributed across multiple systems. At the same time, the study identifies significant untapped potential — in particular through dynamic customer risk classification and the integration of offence-specific risk indicators. A prerequisite for this is that digital sexualised violence against children is anchored as a distinct offence category in risk models, both for private-sector payment service providers and within

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

criminal investigations. Subsuming it under other financial crimes does little to systematically improve detection rates.

Platform architectures are also highly relevant: they create or close structural opportunities for exploitation and its concealment. Monetisation features can generate interaction incentives for perpetrators. When detection and protection mechanisms are simultaneously absent, companies become enablers of sexual violence against children. By applying more comprehensive analytical capabilities, companies should fulfil their child rights responsibility. Considering the grave increase in digital commercial exploitation and the massive consequences for those affected, higher protection standards should also be anchored in regulation.

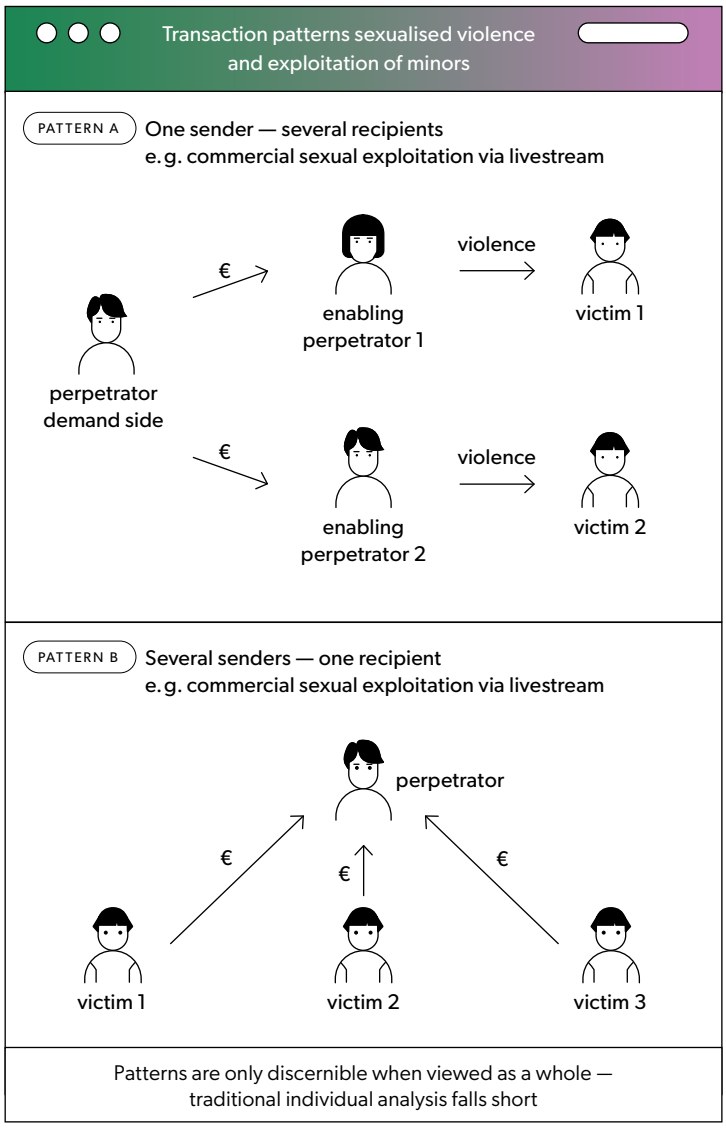


✓ A single, specific amount

✓ Recipient clearly identifiable

✓ Transparent purpose

✓ A standard channel



Common features of both patterns

⚠ Fragmented micro transactions

⚠ Sequential and reocurring

⚠ Several channels and systems

⚠ Purpose obscured or ambiguous

Recommendations for Action

REGULATORY AND STATE ACTORS

Establish legal certainty for proactively acting financial service providers: Financial institutions that report, delay or block suspicious transactions linked to digital sexualised violence against children must be effectively protected from civil liability claims by affected customers. Statutory liability exemptions – comparable to existing safe harbour provisions in the AML context — are a necessary prerequisite for financial service providers to fulfil their protective responsibility without legal risk.

Interconnect financial market and platform regulation: While financial institutions are already comprehensively integrated into AML / CFT regimes, comparable child-rights-based requirements for the monetary interaction structures of digital platforms are lacking. An integrated regulatory perspective linking both areas is urgently needed.

Address monetisation features as instruments of offending in digital child protection law: The Digital Services Act and the EU Guidelines on the protection of minors currently address monetary aspects primarily from a consumer protection perspective — for example regarding manipulative purchasing incentives or loot boxes. The role of payment, gifting and peer-to-peer functions as infrastructure for sexualised violence remains unaddressed. This gap should be closed through binding child-rights-by-design requirements for monetary interaction features and their inclusion in the risk assessments of very large platforms.

Create legally secure interfaces for data exchange: Regulatory frameworks should actively enable the linking of the complementary data perspectives of financial institutions, platforms and public authorities – through defined interfaces, legally secured exchange formats and cooperation platforms. Public-private partnerships should also be promoted; initiatives such as the Tech Coalition's Lantern Project could, for example, be systematically adapted to European framework conditions.

FINANCIAL SECTOR AND PAYMENT SERVICE PROVIDERS

Introduce sequence-based analytical procedures: Existing monitoring systems should be supplemented by behaviour- and sequence-based analytical models. Fragmented microtransactions and recurring payment sequences only reveal their significance when examined collectively — classical single-transaction analyses fail to adequately capture these patterns.

Strengthen dynamic customer risk classification: Customer risk profiles should be continuously updated and supplemented with offence-specific risk indicators for digital sexualised violence. In their own risk analyses, digital sexualised violence and exploitation of children and young people should be anchored as a distinct offence category — not merely as a sub-category of general financial crime.

Expand cooperation within the analytical ecosystem: Financial institutions must understand their role as part of a broader analytical network and intensify structured cooperation with payment service providers, analytical companies and public authorities to close existing information gaps.

DIGITAL PLATFORMS AND TECHNOLOGY COMPANIES

Embed child-rights-by-design and safety-by-design as development principles: Platform features and monetisation models must be systematically examined to determine whether they create unintended incentives or structural opportunities for exploitation and violence. Child protection must be understood as a design requirement from the outset — not as a corrective measure added after the fact.

Integrate monetary dimensions into safety mechanisms: Interaction and payment processes are functionally connected even when payment processing takes place outside the platform. Contextual information from interactions should be systematically incorporated into moderation and detection mechanisms to identify potential risk structures at an early stage.

Expand network and interaction analyses: Relevant risk patterns often only emerge in the context of interaction networks and recurring behavioural patterns, not at the level of individual content or users. Platforms should develop their analytical capabilities accordingly and contribute to cross-sector knowledge building through structured, consolidated reporting.

CROSS-SECTOR COOPERATION AS A KEY TASK

The challenges described cannot be addressed by any single institution alone. Effective analysis and prevention require the systematic linking of complementary data perspectives — subject to strict compliance with data protection and fundamental rights requirements. Three axes of action are central:

Institutionalise cooperation structures: Existing cooperation formats between the financial sector, platforms and public authorities are often still fragmented and project based. They should be developed into long-term, nationally and internationally coordinated structures.

Develop a shared analytical language and risk indicator framework: Different actors operate according to different assessment logics. Shared training formats, harmonised indicator systems and interdisciplinary analytical approaches are fundamental prerequisites for effective cooperation and cross-sector knowledge generation.

Design regulation adaptively: Digital platforms, payment infrastructures and risk dynamics evolve at high speed. Governance models must be based on continuous monitoring and adaptation in order to effectively respond to structural changes.

This Policy Brief is based on the study ›Kleine Beträge, gravierende Folgen: Finanztransaktionen zur sexuellen Ausbeutung von Minderjährigen im digitalen Raum‹ [›Small Amounts, Grave Consequences: Financial Transactions for the Sexual Exploitation of Minors in the Digital Space‹] by Dirk Findeisen, commissioned by ECPAT Germany. The study combines a comprehensive international literature review with qualitative interviews with actors from law enforcement, financial services and civil society organisations. It is aimed at decision-makers from politics, the financial sector and the platform economy, and identifies where concrete action is required.

EDITORIAL TEAM

Lea Peters (Text)
Antje Monshausen (responsible in terms of press law)

DESIGN

www.studio-nea.de

PUBLISHER

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

NEWSLETTER

www.ecpat.de/newsletter

@ecpatgermany

ECPAT Germany