

HANDLUNGSFELD DIGITALER RAUM

Small Amounts, Grave Consequences

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



ECPAT STUDIE

Foreword

The digital world is now an integral part of everyday life for children and young people. They communicate via messaging services, spend time on social media platforms, play online games and navigate digital spaces that open up opportunities for participation, education and social relationships. At the same time, new forms of risk are emerging here: digital sexualised violence and the exploitation of children are increasing dramatically worldwide in terms of scale, pace and complexity. Worldwide, over 300 million children are currently affected by this every year.¹ In Germany alone, the hotline jugendschutz.net received just under 14,000 reports of sexualised violence against children in the digital space in 2025.²

For years, we have been observing how forms of sexualised violence are changing and are increasingly being facilitated, organised and monetised through digital technologies. What is particularly worrying is the growing economic dimension of this phenomenon. In many cases, financial transactions have now become a key prerequisite and driving force behind digital violence and exploitation – for example, in cases of sexual exploitation via live streaming, financially motivated sexual extortion or so-called "pocket money dates". Even small sums of money can have serious consequences for children, whose vulnerability is systematically exploited in this way.

At the same time, it is apparent that wherever there are flows of money, traces are left behind. Financial transactions can facilitate violence and exploitation, but they can also provide clues to the structures, networks of perpetrators and dynamics of the offences. Yet this relationship has not been researched adequately to date and receives too little attention in political, regulatory and institutional debates. Platforms see interaction data, while financial institutions can identify transaction patterns – yet the two perspectives are still rarely combined in any systematic way. But this is precisely where important starting points for prevention, detection and prosecution can be found.

This is the context in which ECPAT Deutschland e.V. has commissioned this study. The author of the study, Dirk Findeisen, combines international research findings with qualitative interviews, thereby offering a fresh perspective on a pressing yet hitherto neglected area of research. ECPAT maintains that the safety of children and young people must be ensured at all times, including in digital spaces. Decision makers in politics and business are called upon to improve regulations and processes. We hope that this study will help to strengthen cross-sector cooperation and provide concrete incentive for effective child protection.

Antje Monshausen, Managing Director of ECPAT Deutschland e.V.

¹ Childlight (2024). Into the Light Index on child sexual exploitation and abuse globally: 2024 report. Edinburgh: Childlight – Global Child Safety Institute. www.childlight.org/uploads/publications/into-the-light.pdf

² Jugendschutz.net (2026). 2025 Report: Jugendschutz im Internet. Mainz. <https://bericht.jugendschutz.net/jahresbericht-2025>

About the author

Dirk Findeisen is a Senior Advisor on Anti-Financial Crime, Risk Management and Compliance. He looks at the question of how financial crime is evolving in increasingly interconnected and technology-driven systems. Accordingly, he works at the intersection of regulation, technology and data. His focus is on topics such as AI, data governance and cross-border financial flows – and the question of how responsibility and control can be reorganised within modern financial systems.

About ECPAT Deutschland e.V.

ECPAT Deutschland e.V. is committed to protecting children and young people from sexualised violence, exploitation and human trafficking. This alliance of 25 organisations across Germany campaigns against human trafficking, develops measures to protect children in the digital sphere and the tourism sector, and supports the development of child protection policies within organisations and businesses.

As part of the international network ECPAT International, which has over 141 members in 113 countries, ECPAT Germany is committed to measures to combat sexualised violence, exploitation and human trafficking, based on the UN Convention on the Rights of the Child.

Table of Contents

Management summary.....	6
I. Introduction and objectives	9
1.1 Relevance of the study	11
1.2 Scope and target groups	12
1.3 Methodology and structure of the study	13
II. The digital economy and sexualised violence against minors.....	18
2.1 Development of digital markets and platform economies	20
2.2 Digital monetisation and shadow economies	22
2.3 International regulatory and protection frameworks	23
2.4 Overview of global case types and stakeholder structures	25
2.5 Incorporation into the 4Cs typology of online risks	28
III. Financial structures and mechanisms in the context of sexualised violence...29	
3.1 Transaction and payment mechanisms	30
3.2 Economic and technical dynamics of financial flows	36
3.3 Key stakeholders and intermediaries	42
3.4 Typologies and red flags	50
3.5 Comparison: Global vs. D-A-CH-specific patterns	58
IV. Results of the empirical analysis.....	65
4.1 Structural analysis using the 4Cs model and financial risk categories....	67
4.2 Patterns identified.....	69
4.3 Links between payment methods, anonymity and risk profiles	71
4.4 Typologies and possible thresholds	74
V. Discussion and analysis.....	78
5.2 Implications for AML/CFT frameworks and financial institutions	80
5.3 The role of platforms and digital ecosystems	82
5.4 Limitations of finance-centred analysis.....	83
5.5 Implications for institutional cooperation and governance	85
6.1 Recommendations for the financial sector and payment service providers	88
6.2 Recommendations for digital platforms and technology companies	89
6.3 Recommendations for action for regulatory and government bodies.....	90
6.4 Cross-sector cooperation and data integration.....	92

Appendix.....	94
I. Overview of the expert interviews and written surveys.....	94
II. Methodology and data documentation	94
Bibliography.....	98

List of Figures

Figure 1: Conceptual framework.....	14
Figure 2: Simplified system model	27
Figure 1: Comparison of payment infrastructures	36
Figure 2: Key stakeholders	44
Figure 3: Visibility of relevant data.....	49
Figure 4: International standards & national implementation	61
Figure 5: Digital interaction, monetisation and financial analysis.....	66
Figure 6: Platform context, monetisation and detectability	77

List of tables

Table 1: Institutional levels of monitoring digital financial transactions	43
Table 2: Comparison of institutional models of selected FIUs.....	64
Table 3: Classification of digital payment infrastructures.....	73

Management summary

Digital interaction spaces, platform economies and new payment infrastructures have led to communication, monetisation and financial transactions becoming increasingly intertwined in recent years. This development opens new opportunities for economic activity and interaction. At the same time, however, it also presents growing challenges for the analysis and prevention of digital exploitation and patterns of violence. This is because criminals – not least sex offenders³ – use digital financial systems to exploit children sexually.

The aim of this study is to analyse financial structures and mechanisms systematically in the context of digital interaction spaces and to assess their significance for financial institutions, platform operators and regulatory bodies. The focus here is on the question of how monetary transactions are embedded in digital interaction processes and what implications this has for existing approaches to analysis and governance.

The study is based on a qualitative, two-stage analysis:

- Review of international studies and status reports
- Interviews with experts from financial institutions, payment service providers, block-chain analysis firms, law enforcement agencies, financial intelligence units, technology organisations and NGOs
- The recommendations developed from this study were also discussed and refined at an interdisciplinary symposium ("Follow the Money – Financial Transactions and Sexual Violence against Children and Young People") attended by representatives from the financial sector, regulatory bodies, law enforcement, academia and civil society. The challenges and proposed solutions identified there confirm key findings of the study and supplement them with practical perspectives on implementation barriers and institutional frameworks.

The interview responses were first recorded in a structured matrix and then consolidated into cross-source structural patterns and typologies. This approach enables a systematic analysis while ensuring the anonymity of the interviewees.

Key findings:

- 1. The financial dimension as a structural feature of digital exploitation.** Digital technologies have fundamentally changed the commercial dimension of the sexual violence and exploitation of minors. Nowadays, financial transactions form an integral part of an ever-widening range of criminal offences – from exploitation and monetised live streaming to financially motivated sexual extortion (FMSE).
- 2. Monetisation as an integral part of digital interaction spaces.** Monetary transactions rarely occur in isolation in the digital space. Rather, they are closely linked to communication and interaction processes and are often embedded in platform structures.
- 3. Recurring structural patterns in financial interactions.** The analysis identifies several key patterns that point to transactions involving the sexual exploitation of minors. However, their significance often only becomes apparent when several transactions and pieces of contextual information are considered together:

- a. Fragmented microtransactions and sequential payment structures
 - b. Platform-based monetisation models
 - c. Cross-platform interaction and payment structures
 - d. Hybrid payment methods (combination of different infrastructures)
- 4. Fragmentation of data perspectives.** No single institution has a complete picture of the situation. A key structural problem is that relevant information is held by different parties:
- a. Platforms monitor interactions and can identify networks
 - b. Financial institutions monitor transactions
 - c. Government bodies aggregate partial perspectives
- 5. Limitations of traditional transaction monitoring systems.** Traditional transaction monitoring systems for the detection of AML/CFT⁴ are limited in cases where transactions are fragmented, contextual information is not available and payment structures are spread across multiple systems – as with sexual exploitation. At the same time, the study shows that existing systems can be improved significantly by further developing risk-based approaches (e.g. dynamic customer risk classification and sequence-based analyses).
- 6. Importance of payment infrastructures and identifiability.** The analysis shows that the traceability of transactions depends largely on the payment infrastructure used. Differences between account-based systems, peer-to-peer services and crypto-based transactions have a significant impact on institutional analytical capabilities – and thus also on the ability to identify transactions that may be linked to the sexual exploitation of minors.
- 7. Strengthening institutional and operational frameworks.** The findings of the symposium make it clear that the effectiveness of existing and future measures does not depend solely on regulatory requirements or technical detection capabilities.

The results confirm key findings from international analyses (including those of the FATF⁵ and Europol), while expanding on them by incorporating the perspective of systematic financial analysis. The study makes a key contribution to:

- establishing the link between the platform economy and financial analysis
- developing structured typologies of monetised interaction patterns
- analysing the institutional fragmentation of data perspectives

The following recommendations for the respective stakeholder groups can be derived from this:

For financial institutions

- Further development of existing AML/CFT systems to enable the detection of criminal acts relating to the sexual exploitation of minors
- Greater consideration of transaction sequences and behavioural patterns
- Integration of additional contextual information on sexualised violence and exploitation of minors into risk assessments

⁴ AML stands for anti-money laundering, i.e. the fight against money laundering. CFT stands for countering the financing of terrorism, i.e. the fight against the financing of terrorism.

⁵ FATF is the Financial Action Task Force, the leading international body for combating money laundering, terrorist financing and the proliferation of weapons of mass destruction.

For platform operators	→ Greater consideration of financial dimensions in security and moderation systems
	→ Integration of the "child-rights-by-design" and "safety-by-design" concepts
	→ Further development of analytical capabilities relating to network structures
For regulatory stakeholders	→ Closer integration of financial and platform regulation
	→ Promotion of cross-sector cooperation models, including improvement and clarification of reporting procedures and reporting criteria through standardisation and provision of updated typology papers, red flag indicators and operational guidelines in the context of sexualised violence and the exploitation of minors
	→ Improvement in the exchange of information between financial stakeholders
	→ Support for pilot projects and empirical research
For all stakeholders*	→ Expansion of cross-sector cooperation
	→ Development of common analytical approaches and data formats
	→ Establishment of integrated governance models that take child protection strategies into account and tackle sexualised violence and exploitation

The study shows that monetary interactions in the digital space can only be understood in terms of the interplay between interaction, platform structure and payment infrastructure.

Effective approaches to analysing and preventing sexualised violence and exploitation of children⁶ therefore require an integrated, cross-sectoral perspective that brings together the previously separate approaches taken by platform and financial systems.

⁶ According to the United Nations Child Rights Convention a child is any person below the age of 18.

I. Introduction and objectives

The ongoing digitalisation of communications, trade and financial services has created new economic and social spheres of activity in recent years. Digital platforms, social networks, instant messaging services and globally available payment systems enable fast, accessible and cross-border interactions. These infrastructures are an integral part of modern societies – yet they can also be misused for criminal purposes. This includes various forms of technology-facilitated sexual exploitation of minors.

Alongside the production, distribution and consumption of such content, financial considerations are increasingly coming to the fore. Monetisation models, digital payment services, peer-to-peer transfers, subscription-based platform structures and cryptocurrencies can contribute to the financing, facilitation or concealment of sexualised violence and exploitation both directly and indirectly. Particularly in the context of exploitation, organised perpetrator structures and financially motivated sexual extortion, cash flows are becoming increasingly important as an analytical tool.

At the same time, such financial transactions are often characterised by relatively low transaction volumes but have the potential for significant individual and societal impact (low volume – high impact). This poses particular challenges for financial institutions, supervisory authorities and law enforcement agencies: on the one hand, sensitive and nuanced detection mechanisms are required; on the other, measures must remain proportionate, legally sound and technically feasible.

While the criminal law, criminological, media education and social science dimensions of sexualised violence against minors have been the subject of intensive research, the specific role of financial transactions has so far been examined less systematically.⁷ Although several international studies in recent years have addressed the financial aspects of digital sexualised violence against minors, there has so far been little in the way of a consistent, interdisciplinary synthesis that systematically brings together technical, financial, forensic, regulatory and criminological findings and assesses their practical applicability – particularly in German-speaking countries – for prevention, detection and cooperation.

Against this background, the aim of this study is to conduct a structured analysis of the role of financial transactions in the context of sexualised violence and exploitation against minors in the digital space. It develops a systematic classification of relevant monetisation mechanisms, transaction patterns and institutional interfaces, and examines which financial indicators may arise in different criminal contexts. Furthermore, the study examines existing cooperation frameworks between the financial sector, law enforcement, platform operators and social

⁷ The works are categorised as follows:

Criminal law / legal policy / regulation

- Witting, S.K. (Leiden University, doctoral thesis): Child sexual abuse in the digital age: Rethinking legal frameworks and transnational law enforcement collaboration, Leiden, 2020.
- RESPECT International (Legal Analysis): Regulation of Child Online Sexual Abuse – Legal Analysis of International Laws & Comparative Legal Analysis, 2020.
- Council of Europe – Lanzarote Convention (Explanatory Report): Overview and analysis of the key European legal instrument against the sexual exploitation and sexual abuse of children, Brussels, 2024.
- European Parliament Research Service (Briefing): Combating child sexual abuse online, Brussels, 2026.

Criminological / police & security agency status reports

- Europol (Report): Exploiting Isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic, Brussels, 2020.
- UNODC (Cybercrime Module / Educational Material): Online child sexual exploitation and abuse,

Social sciences / Epidemiology / Prevalence / Risks / Impact

- Fry, D. et al (Lancet Child Adolescent Health) Prevalence estimates and nature of online child sexual exploitation and abuse: a systematic review and meta-analysis, Online Publication, 2025
- Schnittenhelm, C. et al (Adolescent Research Review): Cybergrooming Victimization Among Young People: A Systematic Review of Prevalence Rates, Risk Factors, and Outcomes, 2024, <https://doi.org/10.1007/s40894-024-00248-w>.
- Ringenberg, T.R. et al (Grooming strategies): A scoping review of child grooming strategies: pre- and post-internet, 2022, <https://doi.org/10.1016/j.chiabu.2021.105392>
- Page, S. et al (Child Abuse Review): Psychological and Emotional Harms of Online Child Sexual Exploitation and Abuse in Children Under the Age of 18: A Systematic Review of the Evidence; Edinburgh, 2025

Media education / Prevention / Awareness / Interventions

- Patterson, A., Ryckman, L. & Guerra, C. A Systematic Review of the Education and Awareness Interventions to Prevent Online Child Sexual Abuse, *Journal of Child Adolescent Trauma* 15, 857–867 (2022). <https://doi.org/10.1007/s40653-022-00440-x>
- Smahel, D. et al (Survey report): EU Kids Online 2020 – Survey results from 19 countries, Kids Online, 2020, [10.21953/lse.47fdeqj01ofo](https://doi.org/10.21953/lse.47fdeqj01ofo).
- Livingstone, S./Stoilova, M. (4Cs framework): The 4Cs: Classifying Online Risks to Children, Hamburg, 2021

organisations, and identifies areas for appropriate further development of prevention and detection mechanisms.

The study combines a global perspective with an in-depth examination of the German-speaking region in order to provide a comparative analysis of international developments, regulatory frameworks and national characteristics. It adopts an interdisciplinary, mixed-methods approach that combines qualitative and quantitative secondary analyses with guided interviews with experts in the fields of law enforcement, finance, technology, forensics and civil society. By systematically triangulating these perspectives, the aim is to provide an empirically sound yet practice-based analysis of this subject area.

The study begins by explaining in more detail its relevance (Section 1.1), its scope and the target groups addressed (Section 1.2). The methodology and structure of the study (Section 1.3) are then set out in detail.

1.1 Relevance of the study

Sexualised violence against minors in the digital world poses a significant challenge to society. It touches on fundamental rights, in particular the right of children to protection from violence and exploitation. The long-term psychological, social and legal consequences for those affected have been extensively documented and highlight the need for effective prevention and intervention measures.⁸ As the digitalisation of various aspects of society progresses, opportunities for crime, channels of communication and dissemination mechanisms are increasingly shifting to digital environments.

International organisations, law enforcement agencies and social organisations have been reporting a quantitative and qualitative diversification of such types of crime for some years. Alongside the dissemination of depictions of sexualised violence against minors, forms of sexual exploitation – such as live-streaming of sexual exploitation and financially motivated sexual extortion (FMSE) – are becoming increasingly prevalent. Digital platforms, messaging services and cloud infrastructures are creating new spaces for establishing contact, coordination and distribution.

At the same time, digital payment and financial infrastructures have developed considerably. Low-threshold peer-to-peer transfers, subscription-based services, platform-integrated monetisation models and the use of cryptocurrencies enable flexible, cross-border and, in some cases, anonymous transaction processing. These developments form an integral part of the digital economy but can also be exploited for criminal purposes. In the context of sexualised violence against minors, the financial dimension can create both direct incentives for monetisation and structural conditions that facilitate such behaviour.

From a regulatory perspective, this area is embedded in various frameworks. International standards on combating money laundering and terrorist financing – particularly those set out by the Financial Action Task Force (FATF) – emphasise the need for risk-based approaches

⁸ Hamilton-Giachritsis, C. et al (2017) "Everyone deserves to be happy and safe": a mixed-methods study exploring how online and offline child sexual abuse affects young people and how professionals respond to it (PDF). London: NSPCC
Schmidt, F., Varese, F., & Bucci, S. (2023). Understanding the prolonged impact of online sexual abuse occurring in childhood. *Frontiers in Psychology*, 14, 1281996. <https://doi.org/10.3389/fpsyg.2023.1281996>

and cross-sector cooperation. At European level, regulatory initiatives in the areas of digital services, platform liability and financial market supervision – such as the Sixth Anti-Money Laundering Directive and the Digital Services Act – are constantly evolving. At the same time, there are national responsibilities assigned to law enforcement agencies, financial supervisory authorities and financial intelligence units, each of which takes a specific perspective on the phenomenon. The fight against sexualised violence against minors in the digital sphere therefore operates at the intersection of child protection, law enforcement, financial market regulation and data protection.

The institutional complexity of this issue requires coordinated cooperation between the financial sector, law enforcement agencies, platform operators, technical service providers and social organisations. Against this background, there is a particular need for a systematic classification of the financial dimension in the context of sexualised violence against minors. Such a classification can help to:

- gain a better understanding of financial risk patterns;
- assess indicators and red flags in a nuanced way;
- identify interfaces for cooperation between relevant stakeholders;
- determine the scope for action in the areas of prevention, detection and regulation.

This study addresses this need and contributes to a structured analysis of the interplay between digital violence, financial mechanisms and institutional frameworks. It sees itself as an interdisciplinary bridge between research, practice and regulation.

1.2 Scope and target groups

The present study adopts an interdisciplinary and practice-based approach; however, it does not claim to be exhaustive or to provide a definitive assessment of all forms of sexualised violence against minors in the digital sphere. The study focuses on analysing the financial aspects of such offences. The study does not aim to provide a comprehensive legal commentary on individual offences, an in-depth analysis of offender profiles, or a detailed assessment of preventative measures in terms of media education. These aspects are taken into account only insofar as they are relevant to an understanding of monetary mechanisms and institutional interfaces.

Furthermore, the study is based primarily on publicly available sources, specialist literature and interviews with experts. It does not make use of operational investigation data, classified information or personal case files. Statements regarding transaction patterns, indicators and cooperation models are therefore made at a structural and typological level, rather than as a comprehensive empirical survey or a statistically representative analysis.

It should also be kept in mind that digital business models, technical infrastructures and regulatory frameworks are undergoing dynamic change. The analysis therefore reflects the state of knowledge available at the time of the study and can only anticipate future developments to a limited extent.

The study does not pursue any normative or political agenda in the sense of specific legislative proposals. Rather, it aims to provide an objective, structured basis for technical discussions and potential further developments in practice and regulation. Recommendations for action are intended as suggestions for discussion, which must be examined and developed within the relevant institutional and legal context.

The study is aimed in particular at:

- Financial sector stakeholders (banks, payment service providers, crypto service providers, compliance and risk management functions);
- Law enforcement agencies and financial intelligence units;
- Supervisory and regulatory authorities;
- Platform operators and technical service providers;
- Civil society organisations working in the field of children's rights;
- Academic and political decision-makers.

By presenting financial mechanisms and institutional interfaces in a structured way, the study aims to promote a shared understanding of the issues and lay the foundations for better cross-sector cooperation.

1.3 Methodology and structure of the study

The present study adopts an interdisciplinary, qualitatively orientated research approach that systematically brings together different perspectives on the financial dimension of sexualised violence against minors in the digital sphere. The aim is to develop a structured, analytically sound and, at the same time, practical understanding of the relevant mechanisms, constellations of actors and cooperation structures.

Given the complexity of the subject area – which encompasses technical, financial, criminological, regulatory and social aspects – a mixed-methods design was adopted. This combines a comprehensive qualitative and quantitative secondary analysis with guided expert interviews from a range of institutional contexts. The methodology is not aimed at conducting a representative survey in the statistical sense, but rather at systematically consolidating existing findings and identifying recurring patterns, typologies and structural relationships.

The study follows an iterative approach in this context: findings from literature and reports have been cross-referenced with practical assessments, and vice versa. This process of triangulation is intended both to validate existing findings and to identify blind spots. The evaluation is carried out using an inductively developed system of analysis and categories, which was further refined in the course of the study.

Figure 1 summarises these relationships in simplified form and serves as a conceptual framework for the following sections.

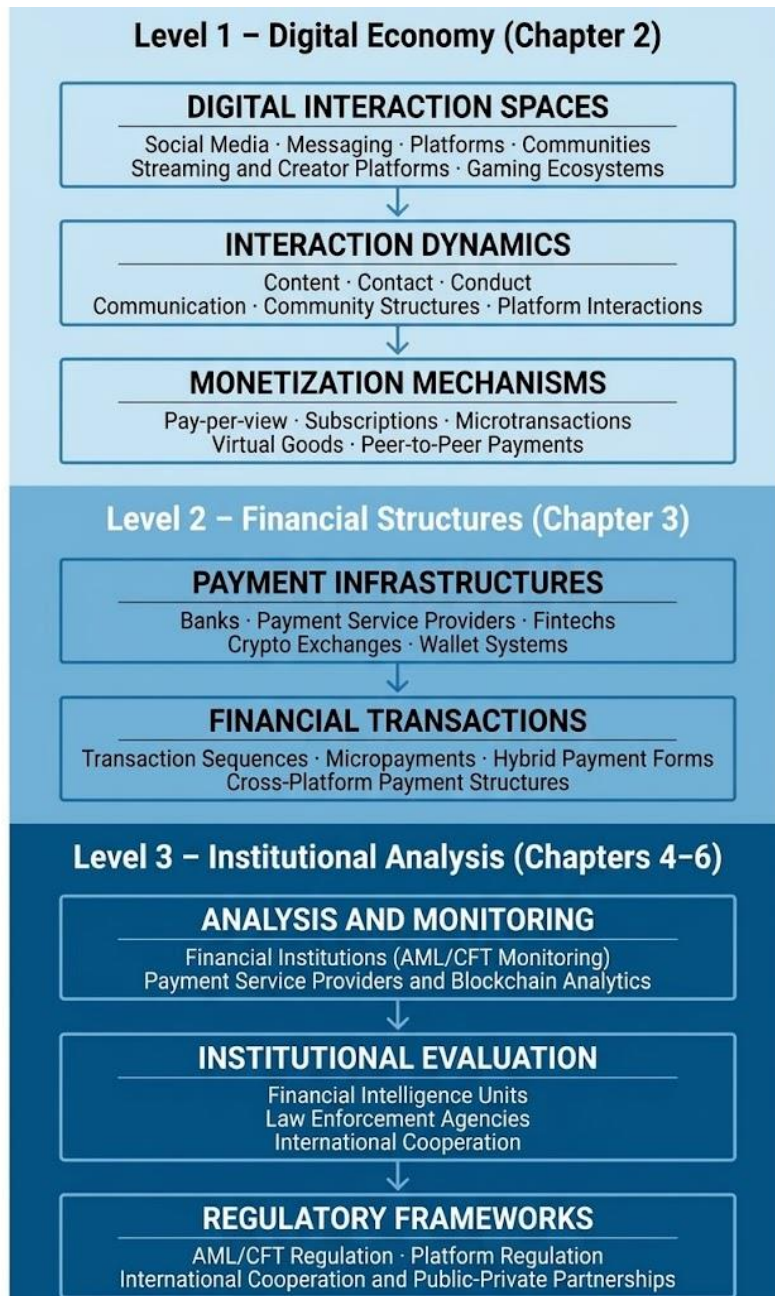


Figure 1: Conceptual framework

The individual methodological components and the structural framework of the study are explained in more detail below.

1.3.1 Qualitative and quantitative secondary analysis

A key component of the study is the systematic review of existing national and international specialist literature, reports, regulatory documents and subject-specific studies. The aim of the secondary analysis was to identify, organise and critically assess the current state of knowledge regarding the financial aspects of sexualised violence against minors in the digital space.

In particular, the following were taken into account:

- International reports and analyses from organisations such as the FATF, Europol, UNODC⁹, and relevant UN and EU institutions;
- Publications by civil society organisations focusing on digital sexualised violence against minors;
- Academic publications in the fields of criminology, law, social sciences, forensics, financial crime and cybercrime;
- Regulatory and supervisory documents relating to anti-money laundering, the regulation of digital platforms and financial market supervision;
- Industry reports relevant to the topic from the finance and technology sectors.

The analysis comprised both qualitative and quantitative elements. From a qualitative perspective, the analysis focused in particular on typologies, definitions of terms, institutional responsibilities and models of cooperation. Quantitative data – such as case numbers, transaction volumes, prevalence estimates and trends – were examined in a comparative way but were not interpreted as a statistically harmonised dataset. Differences in survey methods, approaches to definitions and reporting practices between countries and institutions were taken into account.

The secondary analysis served several purposes: firstly, the conceptual clarification of key terms and types of offence; secondly, the identification of recurring patterns in relation to monetisation mechanisms and types of transaction; and thirdly, the classification of regulatory and institutional frameworks. Furthermore, it formed the basis for the development of the interview guidelines for the primary data collection.

As the available reports sometimes employ different terminology and methodological approaches, a critical assessment of the sources was carried out with regard to their scope, context and wider applicability. The aim was not to reproduce existing findings in isolation, but to place them within a systematic analytical framework.

1.3.2 Primary surveys

To complement the secondary analysis, guided expert interviews were conducted. The aim of the primary survey was to gather practical assessments, empirical findings and institutional perspectives which are only reflected to a limited extent or in aggregated form in publicly available sources.

The interviewees were selected specifically based on the stakeholder groups relevant to the financial dimension. These include:

- Law enforcement agencies and specialist police units;
- Government financial investigation agencies / Financial Intelligence Units;
- Representatives of banks, payment service providers and crypto service providers;
- Compliance and investigations functions in the financial sector;
- Technical and forensic experts;

⁹ United Nations Office on Drugs and Crime

→ International organisations and civil society stakeholders whose work focuses on digital sexualised violence against children.

The interviews were conducted on the basis of structured guidelines, which were adapted to the respective target group. These covered questions relating to observable transaction patterns, monetisation mechanisms, detection logic, institutional interfaces and regulatory and practical challenges. No personal data, operational case information or classified material was collected in the process.

The interviews were analysed qualitatively and thematically. The focus was on identifying recurring patterns, divergent assessments and differences in institutional perspectives. Statements were not interpreted as individual case reports but were incorporated into the overall analysis in aggregated form. Where requested, the contributions were integrated anonymously or in a non-identifiable form.

The primary survey was carried out to:

- reflect on and validate the findings from the secondary analysis;
- identify practical challenges relating to detection and cooperation;
- compile potential "red flag" patterns and institutional interfaces from the perspective of various stakeholder groups.

The interviews therefore provide a qualitative exploration and contextualisation of the findings from the literature, but do not constitute a representative survey.

1.3.3 Systematisation of sources and validation

The findings obtained from the secondary analysis and the primary survey were not considered in isolation but were brought together in a systematic analytical process. The aim was to develop a consistent categorisation system that integrates both theoretical concepts and practical observations.

To this end, the analysed sources were first organised according to key analytical criteria. These included:

- types of offence and contexts in which they occur (e.g. dissemination of depictions of sexualised violence, exploitation, live streaming, financially motivated sexualised extortion);
- monetisation mechanisms and payment methods (e.g. fiat currency transfers¹⁰, platform-based payment models, cryptocurrencies);
- transaction patterns and potential indicators;
- institutional responsibilities and cooperation structures;
- regulatory frameworks.

On this basis, recurring patterns were identified and grouped into thematic clusters. Divergent assessments or contradictory findings from different sources were explicitly taken into account

¹⁰ Cash flows via the traditional financial system (banks, payment service providers, credit card companies, etc.) as opposed to cryptocurrencies or other alternative forms of payment.

and – where possible – contextualised. The aim was not to force everything into a homogeneous picture but to highlight structural similarities and areas of tension.

The findings were validated by means of a multi-stage comparison: findings from the literature were cross-checked against interview responses in order to assess their practical applicability. Conversely, practical assessments were cross-checked against existing reports and studies to minimise potential distortions arising from individual cases. The aim was to achieve mutual validation in this way. In doing so, a conscious decision was taken not to apply a quantitative weighting to individual sources. Rather, the focus was on the analytical coherence of the identified patterns. The study therefore adopts a structuring approach that is not designed to test hypotheses.

This systematic collation and validation of sources is intended to ensure that the typologies, indicators and cooperation models presented are both empirically valid and conceptually consistent.

The study's findings and recommended action points were also presented at an interdisciplinary symposium ("Follow the Money – Financial Transactions and Sexualised Violence against Children and young people", held in Berlin on 29.04.2026) with representatives from the financial sector, regulatory bodies, law enforcement, academia and civil society.

1.3.4 Ethical and linguistic standards

The study deals with a sensitive and potentially distressing subject area. Accordingly, in the design and conduct of the study, particular emphasis was placed on ethical rigour, sensitivity to data protection issues and the responsible use of language.

The design is based on recognised professional guidelines in the field of child protection. Terms are used precisely, in context and without relativising them. The study avoids language that is sensationalist, stigmatising or trivialising. The focus is on structural, institutional and systemic interrelationships rather than on the presentation of specific cases or explicit content.

No personal data was collected or processed in the context of the primary data collection. Unless they had given their express consent to be named, interviewees were anonymised or included in a form that did not allow them to be identified. No operational details relating to ongoing proceedings, no classified information and no sensitive case-specific data were included in the analysis. Furthermore, care was taken not to present identified transaction patterns or technical configurations in a way that might reveal detailed operational information or be open to potential misuse. The analysis remains at an abstract, typological level and deliberately refrains from setting out specific scenarios in operational terms.

The study is intended as a contribution to an objective, evidence-based and responsible examination of the financial aspects of sexualised violence against minors in the digital sphere.

II. The digital economy and sexualised violence against minors

Over the past two decades, the spread of digital technologies has brought about far-reaching structural changes in the economy, communication and social interactions. Digital platforms, social networks, cloud services, mobile applications and global payment infrastructures have become key components of modern societies. They enable new business models, speed up transactions and lower barriers to market entry. Digital markets are characterised by high scalability, cross-border reach and powerful network effects.

These developments present significant economic and social opportunities. At the same time, however, they are also changing the risk landscape. Platform-based business models, decentralised communication structures and, in some cases, anonymised spaces for interaction can be exploited by criminal actors to transfer existing forms of crime into digital contexts or to develop new methods of committing offences. Sexualised violence against minors is particularly affected by these structural changes.

In the digital space, new ways of establishing contact and coordinating and distributing content are emerging. Content can be disseminated globally in a short space of time, communication networks can be established across borders and digital identities enable perpetrators to adapt their strategies flexibly. At the same time, social, technical and economic dimensions are becoming increasingly intertwined. Platforms serve not only as spaces for communication, but also as marketplaces, distribution channels and payment infrastructures.

Against this background, viewing the digital economy as a framework for analysis is becoming increasingly important. Monetisation models such as subscription-based services, pay-per-view structures, donation or tipping systems, peer-to-peer transfers and cryptocurrencies are an integral part of legitimate digital business models. However, these same mechanisms can also be used for financial transactions or to conceal criminal activities. The line between legitimate infrastructure and misuse is not drawn by technical systems, but by specific actions and contexts.

The types of risk are correspondingly diverse. They range from the commercial distribution of illegal content, through monetisation of livestreaming of sexual exploitation, to financially motivated sexual extortion. Furthermore, digital transactions can also play a role in analogue or hybrid forms of exploitation, for example in so-called "pocket money dates".¹¹ In addition, there are indirect forms of monetisation, such as platform structures financed by advertising and data-driven business models. The digital economy therefore functions not merely as a technical backdrop, but as a framework that shapes the structure of opportunities for action, incentive systems and institutional responsibilities.

Section 2 analyses this structural context in greater detail. First, the development of digital markets and platform economies (2.1) and their monetisation mechanisms and shadow economies (2.2) are outlined. International regulatory and protection frameworks are then examined (2.3), before global case types and stakeholder structures are systematised (2.4). Finally, a theoretical framework is embedded within the typology of online risks (2.5) in order to place the financial dimension within a broader societal context of risk.

While section 2 outlines the structural, normative and phenomenological frameworks of digital violence contexts, Section 3 focuses on an in-depth analysis of specific financial mechanisms, the roles of the various actors and transaction structures.

¹¹ Fuhr, E.; Müller, T. (2025). Taschengeld-Treffen: Sexuelle Ausbeutung von Minderjährigen und die Rolle von Online-Anzeigenportalen. ECPAT Deutschland e.V., https://ecpat.de/wp-content/uploads/2025/08/25_ECPAT_Studie_TG-Treffen_digital.pdf

2.1 Development of digital markets and platform economies

Digital markets have undergone a fundamental transformation since the turn of the millennium. While early internet-based business models were often organised in a linear way, today's landscape is dominated by platform-based ecosystems which, as "multi-sided markets", connect different user groups with one another¹². Platforms create value by coordinating interactions between producers, consumers, advertisers and payment service providers, and by reducing transaction costs.

A key structural feature of digital platforms from an economic perspective is network effects¹³. The value of a platform increases with the number of users on the same or a complementary side of the market. This dynamic fosters rapid scaling, market concentration and the emergence of dominant market players. Platform companies are now among the most valuable companies in the world; their business models are based on high scalability with comparatively low marginal costs for digital services¹⁴.

The global significance of digital platforms is also reflected in macroeconomic indicators. According to the United Nations Conference on Trade and Development (UNCTAD), in recent years a significant proportion of global market capitalisation in the technology sector has been accounted for by a small number of large platform companies¹⁵. At the same time, internet usage has risen sharply worldwide: according to figures from the International Telecommunication Union (ITU), around three-quarters of the world's population used the internet in 2023¹⁶. This development significantly expands potential spaces for interaction and strengthens transnational networks.

Digital markets are also characterised by the increasing integration of different functional areas. Communication, content distribution, identity management and payment processing are often bundled within a single ecosystem. Monetisation is achieved through a variety of mechanisms, including transaction fees, subscription models, structures financed by advertising and data-driven business models.¹⁷ The digital payment infrastructure is a key component of these ecosystems. According to the World Bank's Global Findex, 79 per cent of the world's adult population now has access to a formal financial account, with digital payment methods becoming increasingly important¹⁸.

A key element of modern platform economies is the use of algorithmic systems and artificial intelligence (AI) processes. Data-driven platform models are increasingly relying on machine learning techniques to personalise content, optimise recommendation systems, and enable automated moderation and fraud detection. At the same time, these technological systems pose new challenges in terms of transparency, governance and trust, which are addressed in

¹² Rochet, J.-C., & Tirole, J. (2003). Platform Competition in Two-Sided Markets, *Journal of the European Economic Association*, Volume 1, Issue 4, 1 June 2003, pages 990–1029, <https://doi.org/10.1162/154247603322493212>

¹³ Katz, M., & Shapiro, C. (1985). Network Externalities, Competition and Compatibility. *American Economic Review*, <http://links.jstor.org/sici?sici=0002-8282%28198506%2975%3A3%3C424%3ANEACAC%3E2.0.CO%3B2-M>

¹⁴ Parker, G., Van Alstyne, M., & Choudary, S. (2016). *Platform Revolution*. W. W. Norton

¹⁵ UNCTAD (2024). 2024 Digital Economy Report. Geneva

¹⁶ International Telecommunication Union (2025). Facts and Figures 2025, ITU

¹⁷ OECD (2024). OECD Digital Economy Outlook 2024 (Volume 1)

¹⁸ World Bank (2021/2025). Global Findex Database

the Organisation for Economic Co-operation and Development's (OECD) AI Principles, which establish a human rights- and values-based approach to AI governance.¹⁹ AI systems enable platforms to analyse large volumes of user-generated content in real time, prioritise interactions and accurately evaluate economically relevant signals – such as willingness to pay or usage intensity.

From an economic perspective, AI-powered systems reinforce key characteristics of digital markets. They enhance the efficiency of matchmaking between market participants, intensify network effects through personalised reach management, and enable highly granular monetisation via targeted advertising and transaction models.²⁰ At the same time, algorithmic decision-making structures contribute to the automation of scaling processes and thereby alter the dynamics of digital value creation.

International organisations point out that AI-based systems present both opportunities for innovation and increased efficiency and new challenges in terms of transparency, oversight and risk management.²¹ When analysing digital ecosystems, it is therefore important to bear in mind that algorithmic control mechanisms are not merely technical tools but form an integral part of economic platform architectures.

The cross-border nature of digital platforms often creates a tension with nationally organised regulatory and supervisory systems. Cash flows, data flows and communication processes span multiple jurisdictions, while responsibilities for law enforcement, financial supervision and data protection remain tied to specific territories. This structural asymmetry presents both businesses and government institutions with complex coordination and compliance challenges, as the Bank for International Settlements (BIS) has noted since 2023.²²

In addition to centrally organised platforms, decentralised and hybrid structures have also emerged, including peer-to-peer marketplaces, encrypted communication services and blockchain-based systems. Such infrastructures can fulfil legitimate economic and social functions; however, under certain conditions, they make it more difficult to trace transactions and identify responsibilities.

The structural characteristics mentioned – scalability, network effects, transnational reach, integrated payment functions and data-driven business models – should be understood in a value-neutral manner. However, they shape the framework within which abusive behaviour may also occur. In particular, the low barriers to market entry, the potential for expanding global reach and the flexible use of digital identities are changing incentive structures and opportunities for action in the digital space. An analysis of sexualised violence against minors in the digital context therefore requires an understanding of these economic and infrastructural foundations. The payment and value creation mechanisms integrated into platform economies form the basis for the monetisation structures analysed in the following section.

¹⁹ OECD (2024). OECD AI Principles; <https://oecd.ai/en/ai-principles>

²⁰ Brynjolfsson, E., & McAfee, A. (2014). *The Second Machine Age*, and also: Parker, Van Alstyne & Choudary (2016). *Platform Revolution*

²¹ UNESCO (2021). *Recommendation on the Ethics of Artificial Intelligence*

²² BIS (Bank for International Settlements) (2023 & 2025). *Annual Economic Reports*

2.2 Digital monetisation and shadow economies

The monetisation of digital interactions is a key structural feature of modern platform economies. Digital business models are increasingly based on the conversion of attention, reach, data or content into economic value. In addition to traditional advertising and subscription models, transaction-based revenue models, micropayments, platform-integrated payment systems and peer-to-peer transfers have become particularly well established.²³

In this context, global payments have gained considerable momentum. According to data from the BIS, the volume of non-cash payments has risen significantly worldwide in recent years.²⁴ Mobile payment systems, e-wallets and instant payment infrastructures are recording particularly high growth rates.²⁵ At the same time, virtual assets and blockchain-based transfer mechanisms have established themselves as additional digital value transfer infrastructures, the use of which varies in different regions of the world.²⁶

Digital monetisation mechanisms are characterised by several structural features. Firstly, they enable low-threshold, often cross-border, real-time payment processing. Secondly, payment functions are often integrated directly into communication and content platforms, thereby technically intertwining social interactions and economic transactions. Thirdly, the fragmentation of transactions into very small units (micropayments) enables new revenue models, which may be relevant in both legitimate and illegitimate contexts. These microtransactions may occur particularly in the context of sexual blackmail of minors or monetisation of sexual exploitation of children.

In the economic literature, a distinction is made between the formal economy, the informal economy and the criminal shadow economy.²⁷ While informal markets are not necessarily illegal, they do operate outside regulated structures; the criminal shadow economy, on the other hand, comprises activities that explicitly contravene the law. Digital technologies do not fundamentally alter these distinctions, but they can transform existing structures or give rise to hybrid forms in which legal infrastructures are used for illegal purposes.

International organisations point out that the increasing digitalisation of communication and payment systems presents new challenges for law enforcement, oversight and international cooperation. The United Nations Office on Drugs and Crime (UNODC) describes cybercrime as a cross-border phenomenon in which digital infrastructures are used to commit, facilitate or conceal criminal offences²⁸. In its training modules on online child sexual exploitation and abuse, UNODC also emphasises that digital technologies are transforming traditional forms of crime and enabling new forms of interaction and monetisation.²⁹ The integration of communication platforms and payment infrastructures increases the complexity of investigative and supervisory practices. Fragmented transactions, cross-platform payment flows and the use of virtual assets can affect transparency and traceability. The Financial Action Task Force (FATF)

²³ OECD (2024). OECD Digital Economy Outlook 2024 (Volume 1)

²⁴ BIS (2023). Red Book Statistics – Payment, Clearing and Settlement Systems; https://data.bis.org/topics/CPMI_CT

²⁵ McKinsey (2023). Global Payments Report

²⁶ IMF (2023–2025). Global Financial Stability Report

²⁷ Medina, L/Schneider, F. (2018). Shadow Economies Around the World: What Did We Learn Over the Last 20 Years. IMF Working Paper

²⁸ UNODC (undated). https://www.unodc.org/unodc/en/cybercrime/index_new.html

²⁹ UNODC/E4J (undated). Cybercrime Module 12: Online Child Sexual Exploitation and Abuse, <https://www.unodc.org/e4j/en/cybercrime/module-12/key-issues/online-child-sexual-exploitation-and-abuse.html>

therefore emphasises the importance of risk-based approaches when dealing with new technologies and virtual assets.³⁰

Against this background, digital monetisation should not be viewed as an isolated financial phenomenon, but rather as an integral part of data-driven platform architectures. The ability to derive direct economic value from content, interactions or digital services is changing incentive structures and market dynamics. When analysing sexualised violence against minors in the digital space, it is therefore necessary to examine monetisation mechanisms in conjunction with platform structures, payment infrastructures and regulatory frameworks.

Section 2.2 thus establishes the economic link between the structural characteristics of digital markets (2.1) and the in-depth analysis of specific financial mechanisms and transaction patterns in Section 3.

2.3 International regulatory and protection frameworks

The regulation of digital markets and the protection of children from sexualised violence in the digital sphere are embedded within a complex international system of standards. This includes obligations under international law, criminal law conventions, financial regulatory standards and sector-specific regulations for digital services.

At the level of international law, the UN Convention on the Rights of the Child (CRC) forms the central frame of reference. It obliges countries that are party to it to protect children from all forms of sexual exploitation and sexualised violence.³¹ In addition, the Optional Protocol to the Convention on the Rights of the Child on the "sale of children, child prostitution and child pornography" sets out these obligations to protect children in more detail in the context of cross-border offences.³² In 2021, the UN Convention on the Rights of the Child (CRC) confirmed, through General Comment No. 25, that the rights to protection, participation and empowerment set out in the CRC apply without restriction in the digital sphere and must be implemented.³³ These obligations under international law give rise to state obligations to provide protection and to prosecute offences, which also extend to digital contexts.

At European level, the Council of Europe's Lanzarote Convention provides a key framework for criminal law. It requires signatory states to criminalise certain forms of sexualised violence and exploitation of minors, including those committed via information and communication technologies.³⁴ The Convention also emphasises prevention, international cooperation and the protection of victims. At European Union level, these obligations were implemented in 2011 by the Directive on "combating the sexual abuse and sexual exploitation of children and "child pornography" (2011/93/EU).³⁵ The Directive harmonises definitions under criminal law, the conditions for criminal liability and the range of penalties relating to sexualised violence against

³⁰ FATF (2025). Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers

³¹ United Nations (1989/1990). Convention on the Rights of the Child

³² United Nations (2019). Guidelines on the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography

³³ <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation>

³⁴ Council of Europe (2007). Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention).

³⁵ <https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:32011L0093>

children within the Member States. It is currently being revised: the Commission proposal provides for the inclusion of definitions relating to livestreaming of sexual exploitation and sexually motivated extortion, as well as a general tightening of the measures under criminal law.³⁶ As part of this revision, the terminology is also to be updated: in accordance with the Luxembourg Terminology Guidelines, the term "child pornography" is being replaced by child sexual abuse material (CSAM).³⁷

At the same time, regulatory frameworks have developed which do not stem primarily from child protection law but are nevertheless indirectly relevant. These include the standards for combating money laundering and the financing of terrorism set out by the Financial Action Task Force (FATF). The FATF emphasises that certain forms of online crime, including sexual exploitation of minors, can leave a financial trail and must therefore be incorporated into risk-based supervisory and reporting systems.³⁸ Furthermore, new groups of stakeholders have been integrated into the international supervisory framework with the regulation of virtual assets and virtual asset service providers (VASPs).³⁹ In the 6th AML package, the European Union set up the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA) as the central supervisory authority.

New instruments have also become established in the field of digital platform regulation. The European Union's Digital Services Act (DSA) requires large online platforms to comply with enhanced due diligence obligations, transparency requirements and risk assessments in relation to systemic risks, including those associated with the dissemination of illegal content.⁴⁰ Although the DSA is not specifically limited to sexualised violence against minors, it establishes structural responsibilities for platform operators in dealing with unlawful content and, in particular in Article 28, refers to the protection of the rights of children and the handling of content harmful to minors. As a result, especially very large online platforms and search engines must explicitly take into account the risks to minors – including sexualised violence and exploitation – in, for example, their risk analyses. The guidelines relating to Article 28 DSA suggest potential measures for risk minimisation and prevention for service providers.

In addition, there are international cooperation schemes across sectors. Public-private partnership models, Financial Intelligence Units (FIUs), international police cooperation and multi-lateral initiatives to combat cybercrime are aimed at strengthening the exchange of information and coordinated responses. These cooperative frameworks illustrate that the regulation of digital violence is not solely a matter for criminal law but is also embedded within financial supervision and platform regulation.

Overall, it is clear that the protection of minors in the digital sphere is not an isolated policy area but is embedded within a complex web of children's rights, criminal law, financial market regulation and platform regulation. The various regulatory approaches each pursue specific objectives and employ specific instruments, but they overlap in the context of digital monetisation and communication structures. For the purposes of further analysis, it must therefore be kept in mind that financial mechanisms are framed not only in technical or economic terms,

³⁶ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2024%3A60%3AFIN>

³⁷ <https://ecpat.org/wp-content/uploads/2025/04/Second-Edition-Terminology-Guidelines-final.pdf>

³⁸ FATF (2025). Detecting, Disrupting and Investigating Online Child Sexual Exploitation.

³⁹ FATF (2025). Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers

⁴⁰ European Union (2022). Regulation (EU) 2022/2065 – Digital Services Act

but also in normative and institutional terms. Against the backdrop of this normative and institutional framework, different case scenarios can be distinguished systematically.

2.4 Overview of global case types and stakeholder structures

Sexualised violence against minors in the digital sphere takes various forms, which differ in terms of modus operandi, degree of monetisation, organisational structure and institutional responsibility. International organisations such as Europol, the FATF and UN agencies point out that the scope of digital crime has not only increased in volume but has also become more diverse in recent years.⁴¹

One central category of cases concerns the production, distribution and consumption of images of sexualised violence against minors via digital networks. This content can be disseminated via open platforms, closed group structures or encrypted communication services. The organisational structures range from individuals to loosely networked or structured groups of perpetrators.⁴²

Livestreaming of sexual exploitation

In cases of livestreaming of sexual exploitation, perpetrators use digital communication tools such as chat rooms, video calls or livestreaming features on platforms to commit or watch sexualised violence against children in real time. The perpetrators take on various roles in this process: some are in direct contact with the child concerned, demand that certain actions be taken or intervene actively themselves. In other cases, one person is physically present with the child, while a second person gives instructions over the internet – via chat or video, for example. Multiple perpetrators are often involved, and sometimes several children are affected at the same time. Another key feature is the financial aspect: perpetrators often pay money or provide other forms of financial compensation such as digital vouchers to watch or take part in sexualised violence. This money either goes to the perpetrators, who thus profit financially from the exploitation, or directly to the child concerned.

A second category of cases encompasses forms of sexual exploitation in which digital communication and payment systems are deliberately used to generate financial gain. These include, in particular, livestreaming offences in which interactions can take place in return for payment, as well as other services that are provided digitally and have a monetary element.⁴³ The economic dimension comes more to the fore here, as cash flows are directly linked to the commission of the offence.

⁴¹ Europol (2025). Internet Organised Crime Threat Assessment 2025 (IOCTA)

⁴² See *ibid.*

⁴³ FATF (2025). Detecting, Disrupting and Investigating Online Child Sexual Exploitation

In addition to interaction-based exploitative arrangements, there are cases of dedicated, commercially orientated platform structures designed to disseminate and monetise such content systematically. Such structures may include subscription-based access models, tiered membership schemes or usage-based payment models. International analyses suggest that these platforms are often organised based on a division of labour, separating technical, organisational and financial functions from one another.⁴⁴ Monetisation usually takes place via standard payment service providers or virtual assets, which can leave a financial trail.

Another relevant form of this is financially motivated sexual extortion (FMSE). International reports indicate a rise in the number of cases in this area, particularly those involving the use of social media and direct messaging services.⁴⁵ A characteristic feature here is a combination of establishing direct contact, manipulation or deception and a subsequent demand for money.

Sexual extortion

Sexual extortion refers to the blackmailing or coercion of children and young people into sending sexually explicit or intimate images of themselves – under the threat that existing intimate images of the victims will be made public. One particular form is financially motivated sexual extortion: in this context, children and young people are pressured, using intimate images or images of sexualised violence, into sending money or other financial compensation to the perpetrator(s).

Furthermore, digital payment transactions are also relevant in cases of exploitation where the core offence takes place in the analogue world. This is exemplified by so-called "pocket money dates", during which minors are subjected to sexualised violence and, in return, receive money or material gifts from the perpetrators. Similarly, instrumental exploitation of minors for the purpose of committing criminal offences – in the areas of violent crime, for example, or drug-related crime – can leave digital financial traces. In addition to these primary types of cases, indirect forms of monetisation can also be observed. These include, for example, platform structures financed by advertising that are used to generate reach and disseminate content, or the use of digital infrastructure to facilitate organised criminal activities. In such scenarios, cash flows are not necessarily directly linked to individual pieces of content, but form part of more complex economic networks.⁴⁶

The range of stakeholders is correspondingly diverse. It comprises:

- individual perpetrators who use digital communication platforms;
- loosely organised networks, often with transnational links;
- commercially organised groups that operate based on a division of labour;
- platform operators and technical service providers as infrastructure operators;
- payment service providers and financial institutions that provide the transaction infrastructure;

⁴⁴ See *ibid.*

⁴⁵ Thorn (2024). Trends in Financial Sextortion

⁴⁶ UNODC (undated). Cybercrime Overview

→ government and international bodies responsible for law enforcement, supervision and regulation.

International status reports emphasise that digital crime contexts regularly involve cross-border elements, thereby impinging on different legal systems and institutional jurisdictions.⁴⁷ This applies both to criminal prosecutions and to the assessment of transactions that may involve risk under financial regulatory law.

A key point for the present study is that the case types mentioned cannot be defined solely based on their content-related characteristics but are often characterised by the way they are embedded within digital and economic infrastructures. An analysis of the financial dimension therefore requires an understanding of the specific circumstances of each case and the relationships between the parties involved, without reducing these to individual operational details.

Digital interactions, financial transactions and institutional analytical processes form part of a complex ecosystem in which various technological and organisational levels are interconnected. Communication platforms facilitate interactions between users, while digital payment infrastructures facilitate monetary transactions. Financial institutions and compliance systems analyse these transactions and forward any potentially relevant information to financial intelligence units and law enforcement agencies. Figure 2 shows a simplified system model of these interconnected levels.

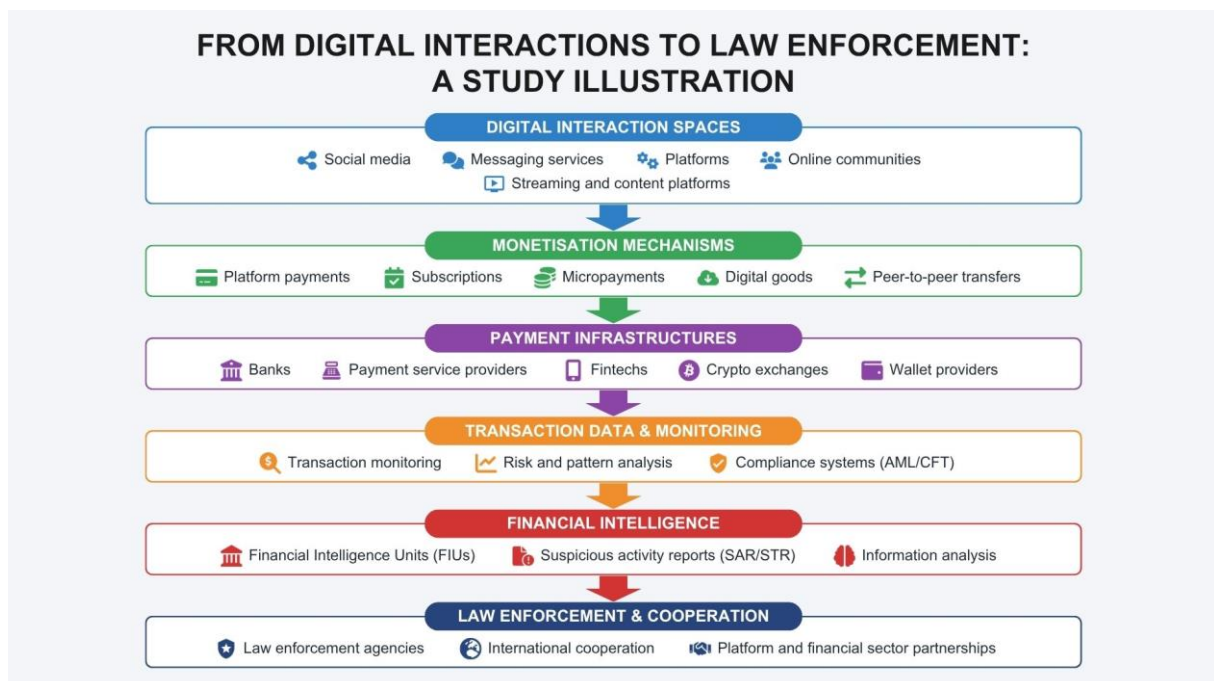


Figure 2: Simplified system model

Section 2.4 thus lays the phenomenological foundations for subsequent incorporation into the 4C model (2.5) and for in-depth analysis of financial mechanisms in Section 3.

⁴⁷ Europol (2023). Internet Organised Crime Threat Assessment (IOCTA)

2.5 Incorporation into the 4C typology of online risks

In international research, the so-called 4C typology of online risks is frequently used to analyse and classify digital risk scenarios. This model, developed by Livingstone and Stoilova, distinguishes between four fundamental dimensions of risk in the digital space: Content, Contact, Conduct and Contract.⁴⁸ Its purpose is to structure online risks systematically and to distinguish between different risk scenarios.

→ The **Content** category covers risks arising from the consumption of problematic or illegal content. In the context of sexualised violence against minors, this relates to the production, distribution and use of such material. The focus here is on the content itself, its accessibility and its distribution via digital platforms.

→ The **Contact** dimension refers to risks arising from interactions between people. These include digital approaches to making contact, grooming processes and manipulative communication strategies. Aspects of monetisation may become relevant in this category if interactions develop into paid arrangements or if financial demands are made.

→ The **Conduct** category covers risks arising from one's own or other people's behaviour in the digital space. These include, for example, sharing or forwarding illegal content and participating in digital group structures. Here, too, financial factors can play a role when behaviour is linked to economic incentives.

→ The fourth dimension, **Contract**, addresses commercial and contractual risks in the digital sphere. These include, amongst other things, non-transparent business models, fraudulent payment demands and monetised interactions. This category is of particular significance for the present study, as it marks the interface between economic infrastructure and digital risk. Monetisation mechanisms can both form an integral part of certain types of criminal activity and create secondary incentive structures.

The 4C typology makes it clear that sexualised violence against minors in the digital space cannot be understood solely as a content issue. Rather, interaction dynamics (Contact), behavioural patterns (Conduct) and economic structures (Contract) are all equally relevant. The financial aspect relates particularly to contact and contract risks, though it is not limited to these.

The preceding sections have shown that digital interaction spaces, monetisation mechanisms and institutional analysis processes are interlinked in a multi-stage system. For the purposes of further analysis in Section 3, this means that financial mechanisms must not be viewed in isolation as a payment phenomenon but must be considered within their respective risk contexts. The 4C typology provides a conceptual framework for this purpose, enabling different manifestations to be compared systematically without reducing them to a single risk category.

⁴⁸ Livingstone, S./Stoilova, M. (4Cs framework): The 4Cs: Classifying Online Risks to Children, Hamburg, 2021

III. Financial structures and mechanisms in the context of sexualised violence

In many cases, phenomena of digital violence are not merely conveyed through communication or content but are also embedded in monetary structures. Cash flows may form a direct part of the commission of the offence or act as accompanying mechanisms that facilitate or incentivise it.

The analysis of financial structures serves several purposes. Firstly, the relevant transaction and payment mechanisms through which financial transactions can be processed should be examined systematically. Secondly, it is important to understand the economic and technical dynamics that shape these payment flows, including economies of scale, transaction fragmentation and cross-border settlement. Thirdly, the stakeholders and intermediaries involved can be categorised according to their respective roles within the financial and platform architecture. On this basis, typical risk patterns and indicators can be systematised, before concluding with a comparison of global trends with specific manifestations in the German-speaking world.

The financial dimension is not viewed in isolation but is understood as an integral part of complex digital ecosystems. Payment mechanisms are embedded in communication platforms, hosting structures, data architectures and regulatory frameworks. Accordingly, the analysis is interdisciplinary in nature and takes into account financial, technical, regulatory and criminological perspectives.

3.1 Transaction and payment mechanisms

The analysis requires a systematic differentiation of the available payment infrastructures. Transaction mechanisms can be categorised in several dimensions:

- Legal and regulatory level (regulated fiat systems, payment service providers, virtual assets);
- Degree of traceability and transparency;
- Speed and fragmentation of transactions;
- Degree of integration into platform or communication systems;
- Cross-border usability.

The following section outlines key categories of payment and transaction mechanisms: traditional fiat-based payment systems, digital payment service providers and e-wallets, peer-to-peer and micropayment systems, virtual assets, and platform-integrated monetisation models. The aim is to set out the respective infrastructural characteristics, regulatory frameworks and functional features, without prejudging specific risk typologies or indicators.

3.1.1 Traditional fiat-based payment methods

Traditional fiat-based payment systems continue to form the backbone of the global financial system. These include bank transfers, direct debits, credit and debit card payments, and cross-border transactions between correspondent banks. These forms of payment are based on government-issued currencies and are generally subject to a comprehensive regulatory framework covering prudential supervision, anti-money laundering legislation and consumer protection.

Structurally, fiat-based systems are characterised by institutionalised intermediation. Transactions are processed through regulated financial institutions or payment service providers,

which are subject to identification, documentation and reporting requirements. In many jurisdictions, they are obliged to report suspicious transactions to the relevant Financial Intelligence Units (FIUs) and to maintain risk-based monitoring mechanisms.⁴⁹ This generally results in greater transparency compared with informal or unregulated forms of payment.

A key feature of traditional fiat systems is their integration into formal identity and due diligence obligations. Opening an account and issuing a card are usually associated with Know-Your-Customer (KYC) procedures. This means that, as a matter of principle, there is a link between the payment transaction and the identified natural or legal person. However, the effectiveness of these mechanisms depends on the quality of identity verification, risk assessment and international cooperation between supervisory and law enforcement authorities.⁵⁰

In the context of sexualised violence against minors, fiat-based payment methods may be particularly relevant where monetary payments are exchanged directly between identifiable account holders or where standard payment infrastructures are used to process digitally facilitated services. The fact that they are subject to a high degree of regulatory oversight does not mean that misuse is impossible, but it does mean that there are institutional frameworks in place for supervision and investigation.

In a typical bank-to-bank transfer, the following elements can be broadly distinguished:

- 1. Initiation by the client**
- 2. Verification by the sending institution**
- 3. Forwarding via clearing and settlement infrastructures**
- 4. Receipt and re-verification by the receiving institution**
- 5. Documentation and storage**

This structure illustrates that, in centralised fiat systems, several intermediaries are involved in the payment process. In addition to the pure transfer of funds, this creates institutional links for identity verification, transaction monitoring and, where appropriate, reporting of suspicious activity to the relevant authorities. Traceability does not stem solely from the existence of account data, but from the combination of identity information, transaction histories and regulatory reporting requirements. At the same time, the involvement of several intermediaries can lead to complex transaction chains, particularly in the case of cross-border payments. Correspondent banking relationships and multi-tier clearing channels generate additional data points but may also reduce transparency for the individual parties involved if information is fragmented.

3.1.2 Payment service providers and e-wallets

Alongside traditional bank-to-bank transactions, digital payment service providers and e-wallet systems have established themselves as a distinct form of intermediation over the past two decades. Some of these providers operate as regulated payment institutions, others as e-

⁴⁹ FATF (2023). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (FATF Recommendations)

⁵⁰ BIS (2018). Sound Practices: implications of fintech developments for banks and bank supervisors

money institutions, and others still as hybrid platforms with integrated payment functions. Their business models are based on simplifying, speeding up and globalising payment processes.

Structurally, these systems differ from traditional financial institutions in that they often act as an additional layer of intermediation between the bank account and the end user. Users provide their bank details, credit card details or other payment methods to a payment service provider, which facilitates transactions technically and, in some cases, also handles account management functions itself. This results in a multi-tiered architecture comprising end users, payment service providers/wallet providers, linked banking or card systems and the receiving payment infrastructure. This structure can speed up transactions and simplifies cross-border settlements, as payment service providers often operate their own internal clearing systems. Transfers can sometimes be carried out internally within the same provider without initiation of a traditional bank-to-bank transfer for every transaction.

A key feature of digital payment service providers is their integration into platform ecosystems. Payments can be integrated directly into social media platforms, marketplaces, streaming services and digital service sites. As a result, communication and payment processes are more closely intertwined than in the traditional banking system. Monetisation models – such as subscriptions, in-app purchases, tipping or donation features – can be processed directly via wallet infrastructures.

From a regulatory perspective, payment service providers in many jurisdictions are subject to anti-money laundering due diligence obligations, including identity verification, transaction monitoring and obligations to report suspicious activity.⁵¹ However, the scope of the regulatory requirements may vary depending on the business model, licence type and threshold. Different risk profiles may arise, particularly in the case of smaller amounts or simplified identification procedures.

Distinctive features of wallet systems from an infrastructure perspective

- Speed: transactions often take place almost in real time.
- Fragmentation: small amounts can be transferred efficiently.
- Cross-border reach: many providers operate internationally.
- Proximity to the platform: payment functions are integrated directly into digital interactions.

When analysing financial structures in the context of sexualised violence against minors, it is important to note that wallet-based systems act as a bridge between the formal financial infrastructure and platform-based interaction. They enable commercial exploitation of digital content and services in direct conjunction with communication processes. At the same time – depending on the regulatory framework and the design of the internal control mechanisms – there are institutional links to monitoring and reporting systems.

⁵¹ FATF (2023). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (FATF Recommendations)

3.1.3 Peer-to-peer transfers and micropayment systems

Peer-to-peer (P2P) payment systems and microtransaction-based models represent another form of digital payment infrastructure. They enable instant money transfers between individuals, often via mobile apps or functions integrated into platforms. Technically, these systems can be based on traditional bank accounts, e-money accounts or hybrid wallet structures. A characteristic feature is the simplification of the payment process from the user's perspective, for example through the use of telephone numbers, email addresses, QR codes or usernames as identifiers.

Structurally, P2P systems are characterised by a high transaction frequency, low individual transaction amounts and a simplified user interface. Many systems are designed for real-time transfers or use internal clearing systems to process transfers without delay. This lowers the threshold for one-off or recurring payments. A key feature of micropayment systems is the fragmentation of amounts. From a technical point of view, even very small amounts can be transferred efficiently without transaction costs reaching a level that makes small transactions economically unattractive. The growing prevalence of instant payment infrastructures is reinforcing this trend.⁵²

Provided that P2P systems are operated via regulated institutions or licensed payment service providers, regulatory oversight generally remains in place. However, simplifying the user interface may mean that complex intermediation and verification processes are not visible to end users. The intermediation chain remains functionally intact, albeit in a more abstract form.

3.1.4 Virtual assets and crypto-based transaction systems

Virtual assets and blockchain-based payment systems constitute a distinct category of digital value transfer. They are based on distributed ledger technology (DLT), in which transactions are validated in a decentralised way and are permanently documented. Cryptocurrencies such as Bitcoin and Ethereum act as digital units of value, which are transferred via cryptographically secured networks.

In blockchain-based systems, transactions can be validated by a decentralised network. In this context, the immediate flow of funds is not necessarily tied to traditional financial institutions. A distinction must be made between different forms of use here:

→ **Custodial models:** Users hold their virtual assets via central service providers (e.g. crypto exchanges or wallet providers), which have custody, identification and, in some cases, monitoring functions. In such scenarios, there are regulatory points of reference, particularly where providers are licensed as Virtual Asset Service Providers (VASPs).⁵³

→ **Non-custodial models:** Users keep their private keys themselves. Transactions take place directly between wallet addresses, without the need for a central intermediary. The intermediation structure is technically simplified here; regulatory touchpoints are shifted to entry and exit points between fiat and crypto systems ("on- and off-ramps").

⁵² BIS (2024). Linking fast payment systems across borders: governance and oversight – Final report to the G20.

⁵³ FATF (2025). Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers

A key feature of crypto-based systems is their pseudonymous address structure. Transactions are recorded publicly on the blockchain but are not directly linked to a legal identity. Transparency arises here at the protocol level (public ledgers), not at the institutional level (customer accounts). The link between a wallet address and a natural person depends on additional information, such as identification procedures carried out by service providers. Furthermore, transactions in crypto-based systems can be carried out across borders and without the need for traditional clearing stages. The processing speed varies depending on the network architecture and load. Certain technical services, such as mixing or privacy mechanisms, may affect the traceability of transaction paths, but without, fundamentally eliminating the existence of a public transaction record.⁵⁴

From a regulatory perspective, international bodies such as the Financial Action Task Force (FATF) have developed guidelines on the integration of virtual assets into existing AML/CFT regimes. In particular, the so-called "Travel Rule" obliges certain service providers to disclose sender and recipient details for transactions exceeding defined thresholds.⁵⁵ However, the specifics of implementation vary from one jurisdiction to another.

When analysing financial mechanisms in this context, it is crucial to recognise that crypto-based systems can exhibit varying degrees of centralisation. There are significant structural differences between fully decentralised peer-to-peer transactions and heavily regulated centralised exchanges, which must be taken into account in a nuanced way as we go on to examine the dynamics, the roles of different stakeholders and the risk patterns.

3.1.5 Platform-integrated monetisation models

Alongside traditional payment and wallet systems, platform-integrated monetisation models have established themselves as a distinct form of digital value transfer. In these scenarios, payment functions are directly embedded in communication, content or interaction platforms.

From an economic perspective, these models can be seen as a further development of multi-sided platform architectures, in which payment services function as part of a comprehensive digital ecosystem.⁵⁶ Platform operators integrate payment functions to reduce transaction costs, increase user retention and support data-driven business models.⁵⁷ Monetisation is achieved through a variety of instruments, including:

- subscription-based access;
- usage-based charges;
- virtual goods or credits;
- "tip" or gift functions;
- digital memberships or premium models.

⁵⁴ BIS (2023). FSI Insights on policy implementation No. 49 – Crypto, tokens and DeFi: navigating the regulatory landscape

⁵⁵ FATF (2025). Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers

⁵⁶ BIS (2019). Big Tech in Finance: Opportunities and Risks

⁵⁷ BIS (2025). Working Paper No 1306 – Big Techs, Credit, and Digital Money

From a technical perspective, these payments are often processed via integrated billing systems, such as those that are standardised in mobile app ecosystems.⁵⁸ In such systems, platform operators can define virtual products, manage recurring subscriptions or provide consumables, which are purchased directly within the application.⁵⁹ The payment itself is usually processed via registered payment methods (e.g. credit card, bank account or digital wallet), while the platform manages the internal settlement and user allocation.

A structural feature of these models is the use of virtual currencies or credits that can be used within the respective ecosystem. Consumer protection and regulatory authorities have repeatedly pointed out that such premium currencies can give rise to complex pricing structures, as real currency units are converted into internal tokens.⁶⁰ From an infrastructure perspective, this means that an additional accounting layer is introduced between external payments and internal value transfers.

In this case, the intermediation structure is functionally bundled. Consequently, in platform-integrated systems, communication, identity and payment data can be consolidated within a single organisational unit. Although payment processing is usually carried out by regulated institutions, it is the platform operator who controls the monetisation logic. This close integration of interaction and payment data is a defining feature of digital platform ecosystems.⁶¹

Another structural aspect concerns the linking of microtransactions to social interactions, for example in the context of livestreaming or community platforms. Studies of digital ecosystems show that virtual gifts or tipping mechanisms can act as key monetisation tools, with interaction and payment taking place almost simultaneously.⁶² This is supported technically by internal wallet systems or real-time settlement.

From a regulatory perspective, a distinction must be made between the role of the payment service provider and that of the platform operator. While payment processing and management of funds are generally subject to anti-money laundering requirements, platform operators may also fall under specific digital or consumer protection regulations, depending on their business model. The specific arrangements depend on the type of licence, the jurisdiction and the organisational structure.

A key factor for the present analysis is that platform-integrated monetisation models effectively blur the boundaries between communication, distribution and payment. In this context, the economic exploitation of digital interactions does not take the form of an external transfer transaction but rather forms part of an integrated system architecture. This gives rise to specific combinations of data availability, extent of intermediation and regulatory points of reference, which differ structurally from traditional fiat or purely peer-to-peer systems.

⁵⁸ Apple Inc. (undated). In-App Purchase Types – App Store Connect Reference; <https://developer.apple.com/help/app-store-connect/reference/in-app-purchases-and-subscriptions/in-app-purchase-types>

⁵⁹ Google LLC (undated). Integrate the Google Play Billing Library; available here via Android Developers: <https://developer.android.com/google/play/billing/integrate?hl=de>

⁶⁰ EU CPC Network (2025). Key Principles on In-Game Virtual Currencies, Ref Ares(2025)2303808; and also: BEUC (2024). Monetising Play – Regulating In-Game and In-App Premium Currencies.

⁶¹ BIS (2019). Big Tech in Finance: Opportunities and Risks

⁶² Ueki, S., Toriumi, F., Sugawara, T. (2024). Game-theoretic implications for identifying the effects of virtual tipping in complex user networks. *Appl Netw Sci* 9, 44 (2024). <https://doi.org/10.1007/s41109-024-00655-x>

Below is an overview of the payment infrastructures:

Category	Identifiability	Institutional Observability	Platform integration	Typical features	Relevance for financial investigations
Classic fiat systems	High	High	Low	KYC, AML monitoring, reporting obligations, central intermediaries	Good traceability, institutional links are in place
Payment service providers & e-wallets	Medium to high	Medium to high	Medium to high	Fast payments, international reach, additional layer of intermediation	Link between financial system and platform economy
P2P & micro-payment systems	Medium	Medium	High	High transaction frequency, low individual amounts, real-time transactions	Patterns often only recognisable at network or sequence level
Virtual assets/crypto	Low to medium	Low to medium	Low	Pseudonymity, on/off-ramps, blockchain transparency	Analysis via network, wallet and transaction patterns
Platform-integrated monetisation	Medium	Medium	Very high	Convergence of interaction, communication and payment	Highly relevant interface between platform and financial data

Figure 3: Comparison of payment infrastructures

3.2 Economic and technical dynamics of financial flows

Payment mechanisms are not static; they only come into their own when interacting with market dynamics, platform architectures, technological characteristics and regulatory frameworks.

Digital financial flows are characterised by specific structural features that distinguish them from traditional, primarily analogue payment processes. These include the high speed of processing, the ability to fragment payment amounts, the global reach of digital infrastructures and the close integration of payment and communication data.

The following analysis is expressly not intended to highlight specific circumvention strategies, operational vulnerabilities or abusive practices. Rather, it aims to describe the structural patterns, economic incentive mechanisms and technological characteristics of digital payment systems. The analytical focus is on systemic dynamics, not on detailed descriptions of individual scenarios that guide action.

The following sections analyse these dynamics in terms of key structural features: fragmentation and transaction granularity, scaling effects in digital markets, transnational shifts in regulatory responsibilities, changes in the structure of intermediation and the integration of payment and interaction data in platform-based ecosystems. The aim is to identify the systemic characteristics of digital financial flows that are relevant for a subsequent analysis of the roles of different actors, risk patterns and institutional response mechanisms.

3.2.1 Fragmentation and transaction granularity

A key structural feature of digital financial flows is the ability to break down payments into many small individual transactions. While traditional payment processes have historically often been characterised by higher transaction costs, time delays or administrative hurdles, digital infrastructures now enable even small amounts to be processed efficiently and at high frequency. Technological developments such as instant payment systems, internal wallet settlements and platform-integrated credit systems have further reinforced this trend.⁶³

From an economic perspective, the possibility of microtransactions lowers the entry barrier for monetary transactions. Small individual amounts may be perceived differently, both psychologically and economically, from larger one-off payments. At the same time, digital systems allow for virtually unlimited repetition of such transactions, which can result in cumulative payment flows without individual transfers, taken in isolation, indicating a high volume.

From an infrastructure perspective, fragmentation leads to a change in the transaction structure. Instead of a few clearly identifiable individual transfers, there may be numerous smaller transfers spread across various times or channels. This is especially the case in platform-based environments where payments are directly linked to interaction events – such as individual pieces of content, messages or digital services.

In technical terms, this development is closely linked to automation of payment processes. Standardised application programming interfaces (APIs), internal ledger systems and real-time processing enable a high level of transaction granularity with comparatively low operating costs.⁶⁴ Fragmentation is therefore not a random characteristic, but the result of specific technological and economic design choices made in digital payment systems.

Compared with the traditional bank-to-bank reference architecture, fragmentation changes the perspective on payment volumes and frequency. While traditional monitoring systems have historically focused heavily on individual transactions involving larger sums, with a high level of granularity the analytical focus may shift towards patterns, sequences or recurring payment relationships.

⁶³ BIS (2024). Linking fast payment systems across borders: governance and oversight – Final report to the G20.

⁶⁴ BIS (2018). Sound Practices: implications of fintech developments for banks and bank supervisors

Furthermore, fragmentation can occur in conjunction with transnationality. Digital infrastructures make it possible to transfer small amounts across borders without fixed cost structures making this economically unattractive. In globally interconnected platform ecosystems, this gives rise to potential international micro-payment flows, the cumulative effects of which exceed those of individual transactions.

For the purposes of this study, fragmentation should therefore be understood as a structural feature of digital financial flows that can influence economic incentives, transaction patterns and analytical valuation logic. It is a key building block in understanding the wider dynamics, particularly in conjunction with economies of scale and platform-based monetisation models. In the context of sexualised violence against minors in the digital sphere, the structural potential for fragmentation can be particularly significant. Monetary transactions can be directly linked to individual digital interaction events, as part of recurring contact or access models for example. The cumulative effect of many small payments can be economically significant, even though individual transactions do not represent a large volume when considered in isolation. For institutional actors, this shifts the analytical focus away from individual transactions and towards sequential or relational patterns.

3.2.2 Scaling and network effects in digital markets

Digital markets are characterised by specific scaling properties that differ significantly from traditional, primarily physical business models. A key characteristic of digital goods and services is the low marginal costs of reproduction and distribution. Once a digital infrastructure is in place, additional transactions or content can be generated and distributed with relatively little extra effort.⁶⁵

This economic characteristic has a reinforcing effect on platform models based on network effects. In many cases, the value of a platform increases in line with the number of its users, as opportunities for interaction, visibility and monetisation potential grow.⁶⁶ Payment functions that are directly integrated into such platforms can benefit from these effects. As reach increases, the volume of monetary transactions also has the potential to rise, without this being accompanied by a proportional increase in infrastructure costs.

From a technical perspective, scalability is supported by automation, standardised interfaces and modular system architectures. Largely digital platforms can carry out payment processes, invoicing and internal settlements automatically. This enables a high transaction frequency while maintaining a consistent operational structure. At the same time, recurring payment models – such as subscriptions or regular small payments – can be managed efficiently from a technical point of view.

Compared with the traditional bank-to-bank reference architecture (3.1.1), the focus shifts from individual, isolated transactions towards systematically recurring payment relationships. While traditional bank transfers are often one-off transactions, digital business models are frequently

⁶⁵ Shapiro, C., & Varian, H. (1998). Information Rules: A Strategic Guide to the Network Economy. *The Journal of Technology Transfer* 25, 250–252 (2000). <https://doi.org/10.1023/A:1007897212472>

⁶⁶ Rochet, J.-C., & Tirole, J. (2003). Platform Competition in Two-Sided Markets, *Journal of the European Economic Association*, Volume 1, Issue 4, 1 June 2003, pages 990–1029, <https://doi.org/10.1162/154247603322493212>

designed with continuity, repeat business and expanding reach in mind. Scaling therefore relates not only to the number of users, but also to the intensity and regularity of financial transactions.

In the context of sexualised violence against minors in the digital sphere, the logic of economies of scale in digital markets can be of particular analytical relevance. Digital communication and platform structures generally enable interaction and distribution processes to be scaled up rapidly. If monetary mechanisms are embedded in such structures, financial flows may also be affected by economies of scale. The economic appeal of individual actions may therefore stem less from the size of individual payments than from the potential for repetition and the reach of digital interactions.

In digital environments, scaling is not linear but is often network driven. For institutional actors such as financial intermediaries or law enforcement agencies, this may mean that risk assessments cannot be based solely on static volume analyses but must also consider growth and reach dynamics.

3.2.3 Transnationality and regulatory asymmetries

Digital payment and platform infrastructures are not, by their very nature, bound by territorial boundaries. Depending on the payment system chosen, financial transactions can be carried out across borders in real time or with minimal delay. This structural transnationality clearly sets digital financial flows apart from banking and payment systems, which have historically had a more national character.

In the standard fiat model (3.1.1), cross-border transactions can be processed via correspondent banking relationships or international clearing systems. While there are extensive regulatory requirements in this area, the involvement of several jurisdictions can nevertheless lead to complex issues regarding responsibilities and information. In the case of digital payment service providers and platform-integrated systems, there is the additional factor that providers, technical infrastructure, users and payment sources are often located in different countries.

In crypto-based systems, territorial allocation is also shifting. Transactions are validated across globally distributed networks, while regulatory access points are often concentrated at so-called on- and off-ramp interfaces between fiat and crypto systems. The geographical location of service providers, wallet providers and exchanges may differ from that of the users. International bodies have therefore emphasised that effective supervision of virtual assets requires cross-border coordination.⁶⁷

Transnationality is not problematic in itself but is rather a defining feature of digital markets. However, it may lead to regulatory asymmetries if various jurisdictions impose differing requirements regarding identity verification, reporting obligations or the level of supervision. Such differences may, from a structural perspective, contribute to financial flows being channelled through systems or locations with specific regulatory characteristics. This analysis

⁶⁷ FATF (2025). Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers

describes this dynamic as an institutional divide, without specifying any concrete alternative strategies or operational configurations.

In the context of sexualised violence against minors in the digital sphere, the transnational structure of digital infrastructures can be of particular relevance. Interactions, content and payment flows may span several countries, while investigative and supervisory powers are typically organised at national level. For institutional actors, this creates a tension between global infrastructure and territorially defined responsibilities. In such circumstances, the effectiveness of prevention and detection measures depends largely on international co-operation, exchange of information and harmonised minimum standards.

From an analytical perspective, transnationality therefore alters not only the geographical dimension of financial flows, but also the structure of institutional responsibilities. In digital markets, payment flows are often embedded in multi-layered, cross-border architectures. For further analysis, it must therefore be borne in mind that regulatory access points, data availability and investigative powers do not necessarily coincide.

3.2.4 Disintermediation and re-intermediation

Digital financial and platform architectures are often characterised by processes of disintermediation, that is, by the reduction or circumvention of traditional intermediaries. Traditional bank-to-bank structures involving multiple institutional oversight bodies can be made functionally simpler through digital payment systems, wallet models or decentralised technologies. From the user's perspective, this makes the payment process seem more straightforward and less complex.

Technically speaking, however, disintermediation does not necessarily mean the complete elimination of intermediaries, but rather, in many cases, their functional reorganisation. In many digital ecosystems, new stakeholders are replacing traditional financial institutions or taking on additional gatekeeper roles. These include, amongst others, payment service providers, cryptocurrency exchanges, wallet providers and platform operators with integrated settlement systems. This process can be described as re-intermediation. Monitoring and control functions do not disappear; rather, they are transferred elsewhere.

This shift affects not only technical processes, but also supervisory and cooperation structures. In digital ecosystems, institutional responsibility is distributed differently from the way it is in the traditional banking system in some respects. While financial institutions have historically played a central role as entities subject to anti-money laundering regulations, a variety of different groups of stakeholders are now integrated into the financial architecture. International standard-setting bodies such as the FATF have taken note of this development and drawn up specific guidelines for new types of intermediaries.

In the context of this study, this dynamic is relevant in that financial flows do not necessarily pass through identical institutional control structures. The transfer of intermediation functions may result in data availability, monitoring processes and reporting obligations being assigned to different parties. In the context of institutional cooperation, this entails the need for a clear understanding of roles and arrangements regarding interfaces. This perspective forms an

essential basis for the subsequent examination of the roles of stakeholders (3.3) and risk patterns (3.4).

3.2.5 Data integration and platform logic

A key structural feature of digital financial architectures is the increasing integration of payment, interaction and usage data within platform-based ecosystems. While in the traditional bank-to-bank model transaction data is primarily processed within the respective financial institutions, in digital platform environments financial transactions are often closely linked to communication, profile and behavioural data.

Platform economies are typically based on data-driven business models in which user interactions, content and transactions are not viewed in isolation, but as interconnected flows of information.⁶⁸ Payment data may contain additional contextual information, such as the frequency of certain interactions, recurring usage patterns or activity patterns on the platform. From a technical perspective, this integration is made possible by centralised data architectures, standardised interfaces and automated analysis systems.

Compared to the traditional reference architecture (3.1.1), this changes the structure of information availability. Whereas in the traditional model, transaction data and communication data are processed separately at an organisational level, platform-integrated systems are able to combine both types of data at a technical level, subject to data protection and regulatory constraints. This opens up potential new analytical perspectives but also brings with it new requirements in terms of governance, transparency and accountability.

At the same time, the concentration of payment and interaction data in individual digital ecosystems can lead to functional centralisation. In such scenarios, platform operators have access to aggregated information that goes beyond the pure payment transaction. International analyses of the role of large technology platforms in the financial sector indicate that this data integration is a key distinguishing feature compared with traditional financial intermediaries.⁶⁹

The relevance to the context of this study stems from the interconnection between communication and payment data, as monetary transactions often do not take place in isolation but in the context of digital interactions. The structural interdependence of interaction and financial flows is changing the perspective on risk analysis and institutional cooperation. At the same time, the use of such data is subject to strict legal and ethical frameworks, particularly with regard to data protection, purpose limitation and proportionality.

This analysis therefore describes data integration as a systemic feature of digital platform economies. It implies neither a general increase nor a reduction in risks but rather highlights the fact that financial flows are increasingly embedded within more extensive data ecosystems. For institutional stakeholders, this may mean that effective prevention and detection strategies require cross-sector cooperation between financial intermediaries, platform operators and supervisory authorities.

⁶⁸ Rochet, J.-C., & Tirole, J. (2003). Platform Competition in Two-Sided Markets, *Journal of the European Economic Association*, Volume 1, Issue 4, 1 June 2003, pages 990–1029, <https://doi.org/10.1162/154247603322493212>

⁶⁹ BIS (2019). Big Tech in Finance: Opportunities and Risks

The dynamics described – fragmentation, scaling, transnationality, shifts in intermediation structures and data integration – do not operate in isolation within digital financial architectures, but rather reinforce one another. Fragmented microtransactions can generate exponential payment flows through platform-driven scaling; transnational infrastructures override institutional responsibilities; and the aggregation of payment and interaction data alters the distribution of control and analytical functions. These structural characteristics are inherent features of digital markets and are not limited to specific contexts of criminal offences. Their relevance to the present study stems from the fact that monetary structures in the digital space should be understood not as linear payment relationships, but as embedded components of complex ecosystems. Financial flows arise, grow and shift within technical and economic frameworks that can redefine institutional points of access.

3.3 Key stakeholders and intermediaries

The payment mechanisms and systemic dynamics described in the preceding sections do not operate in an institutional vacuum. Digital financial flows are embedded in complex networks of stakeholders, within which various institutions perform technical, regulatory, operational and analytical functions. Analysing this division of roles is essential for gaining a nuanced understanding of responsibilities, control points and the need for cooperation.

While in the traditional banking system responsibility under anti-money laundering legislation lay primarily with regulated financial institutions, the landscape of stakeholders in digital ecosystems has become significantly more diverse. In addition to banks, payment service providers, e-money institutions, cryptocurrency exchanges, wallet providers, platform operators and technical infrastructure service providers act as functional intermediaries. At the same time, government bodies such as financial intelligence units, law enforcement agencies and supervisory authorities all operate, each with their own distinct mandates.

The role of a participant is determined less by its formal designation than by its functional position within the financial and data architecture. The key question is whether a stakeholder:

- initiates or facilitates cash flows;
- carries out identity checks;
- stores or analyses transaction data;
- is subject to regulatory reporting requirements;
- has investigative and/or supervisory powers.

Digital markets mean that these functions are not necessarily identical. Payment processing, data processing and regulatory responsibility may be organised separately or combined. The shift in intermediation structures (see 3.2.4) therefore necessitates a systematic clarification of roles, as set out in Table 1.

Institutional level	Typical stakeholders	Observable information	Analytical perspective
Financial institutions	Banks, payment service providers, fintech companies	Transaction data, account information, payment sequences	Identification of unusual transaction patterns and risk-based monitoring systems
Crypto-based financial service providers	Cryptocurrency exchanges, wallet providers, blockchain analytics firms	Blockchain transactions, wallet addresses, on/off-ramp activities	Analysis of transaction networks and blockchain structures
Digital platforms	Social media, messaging services, content and streaming platforms, gaming platforms	Interaction data, user connections, platform activity	Contextualising digital interactions and communication structures
Financial Intelligence Units (FIUs)	National analytical authorities	Suspicious activity reports, aggregated financial information, international FIU data	Pattern recognition across multiple reports and institutional data sources
Law enforcement agencies	Police, public prosecutor's office, specialist investigative authorities	Investigation data, seized information, international mutual legal assistance	Criminal investigations into complex networks and criminal structures
Supervisory and regulatory authorities	Financial supervisory authorities, central banks, EU institutions	Systemic risks, regulatory reports, sectoral analyses	Assessment of regulatory risks and development of institutional frameworks

Table 1: Institutional levels of monitoring digital financial transactions

This institutional dimension is particularly relevant to the present study, as financial transactions often represent only one part of a broader landscape of digital interactions. Effective prevention, detection and cooperation mechanisms therefore require that the roles of the various stakeholders are clearly defined, that interfaces are structured transparently and that information flows are organised in a legally compliant manner.

The following analysis is based not primarily on formal institutional designations, but on functional roles within the digital finance and data architecture. This perspective takes account of the dynamics described in Section 3.2, according to which intermediation, control and analysis functions in digital ecosystems do not necessarily correlate with traditional institutional responsibilities.

Digital payment and platform structures are characterised by forms of organisation based on the division of labour, some of which are transnational. An individual stakeholder may perform several functions, while individual functions may be distributed among different institutions. Payment processing, identity verification, data analysis and regulatory supervision may be organised separately or combined. A purely institution-based approach would fail to reflect these functional overlaps adequately.

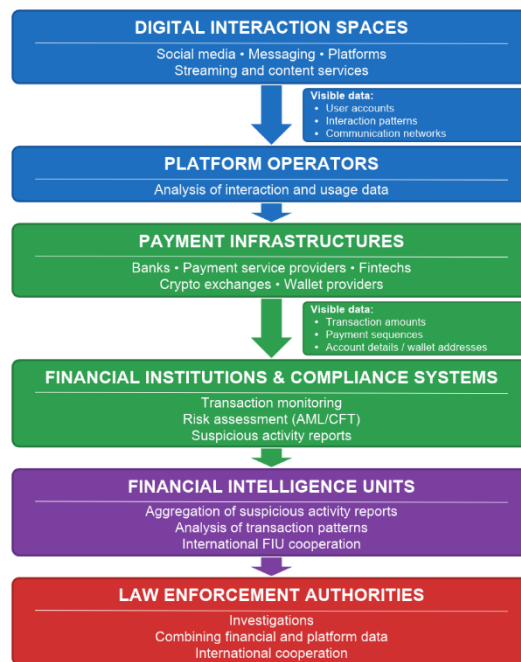


Figure 4: Key stakeholders

Figure 4 illustrates these fragmented observational perspectives within digital interaction and payment ecosystems.

By contrast, the functional role perspective makes it possible to analyse systematically

- where control points arise within the architecture;
- which groups of stakeholders have access to what data;
- where regulatory or criminal procedural powers lie;
- at which interfaces cooperation is required.

At the same time, this approach enhances the international applicability of the analysis. As institutional designations and the allocation of responsibilities vary between jurisdictions, the functional structure provides a comparable analytical basis for both global and DACH⁷⁰-specific contexts (see 3.5).

The following subsections distinguish between key roles within the digital financial and platform architecture and assign relevant groups of stakeholders to them by way of example. The aim is to set out responsibilities, scope for action and structural constraints in a transparent manner, without going into the details of operational arrangements.

3.3.1 Infrastructure and payment intermediaries

Infrastructure and payment intermediaries play a central role within digital financial architectures. They facilitate, process or hold financial transactions and are often the first point of contact for institutions in relation to identity verification, transaction monitoring and regulatory reporting systems. This group of stakeholders includes financial institutions, payment service

⁷⁰ DACH stands for Germany, Austria and Switzerland

providers, e-money institutions, cryptocurrency exchanges and providers of custodial wallet solutions.

The significance of this group of stakeholders in relation to sexualised violence against minors in the digital sphere lies primarily in their role as gatekeepers. Depending on their business model, payment intermediaries hold structured transaction data and identity-related information that may be relevant for identifying atypical payment relationships or payment patterns. At the same time, they are subject to legal restrictions regarding data protection, purpose limitation and proportionality. Their scope for action is therefore shaped by a balance between risk identification, regulatory obligations and the protection of fundamental rights.

The effectiveness of this gatekeeper role depends on several factors: the quality of internal risk assessments, the design of technical monitoring systems, the clarity of regulatory requirements and the ability to cooperate with other stakeholder groups. Particularly in transnational contexts (see 3.2.3), differing regulatory requirements and data access rights can influence an institution's ability to act.

At the same time, it should be emphasised that payment intermediaries do not operate in isolation. Their role within the digital architecture is often intertwined with that of platform operators, technical service providers and government bodies. Reports of suspected offences or risk analyses usually only have an effect when they are coordinated with analytical units and law enforcement agencies. The role of payment intermediaries should therefore be understood as part of a cooperative system as a whole, rather than as that of a sole supervisory body.

3.3.2 Platform and technology service providers

Platform and technology service providers supply the digital infrastructure within which interactions, content and – in many cases – financial transactions take place. This group of stakeholders includes operators of social networks, communication, streaming and gaming platforms, hosting service providers, app ecosystems and other technical infrastructure providers. Their functional role differs from that of traditional payment intermediaries, as they primarily create spaces for interaction in which monetary processes can be embedded.

From a functional perspective, platform and technology service providers have access to specific contextual information. While payment intermediaries primarily process transaction data, platform operators also have access to interaction patterns, communication histories and usage frequencies. This arrangement establishes a distinct role regarding prevention, content moderation and internal risk assessments. In many jurisdictions, platforms are subject to specific regulatory requirements, for example in the areas of platform liability, content moderation or digital consumer protection.⁷¹

In cases of digital sexualised violence against minors, platform and technology service providers are often the first point of contact for reporting incidents, moderation decisions or the removal of unlawful content. However, their role is not limited to matters of content. Where

⁷¹ BIS (2019). Big Tech in Finance: Opportunities and Risks

monetary functions are integrated into platform architectures, financial aspects may also be involved – through subscription models, virtual goods or other monetisation mechanisms for example. The functional interface between interaction and payment data therefore requires a clear delineation of responsibilities vis-à-vis payment intermediaries and government authorities.

At the same time, platform operators are subject to particularly strict requirements under data protection law and fundamental rights legislation. The processing of communication and payment data is subject to strict requirements regarding purpose limitation, transparency and proportionality. The design of internal compliance structures must therefore take into account both preventative objectives and the safeguards for the rule of law. From a systemic perspective, platform and technology service providers play an intermediary role between digital interaction and financial processing. Their position within digital ecosystems makes them key partners for payment intermediaries, analytical bodies and law enforcement agencies, particularly where financial processes are closely linked to digital interaction structures.

3.3.3 Analytical and coordinating bodies

Analytical and coordinating bodies play a key bridging role within the digital financial architecture. They are not usually directly involved in the day-to-day processing of payments, but act as bodies responsible for collecting and analysing data and acting as interfaces between private intermediaries and state investigative authorities. This group of stakeholders includes Financial Intelligence Units (FIUs), international coordination networks such as the Egmont Group, and specialised units at European or international level, such as those operating within Europol.

The primary function of these bodies is to receive, assess and pass on reports of suspicious activity submitted by institutions under a reporting obligation, such as banks, payment service providers and cryptocurrency exchanges. They analyse transaction data for possible links to matters of criminal law and, where appropriate, forward the information to the relevant law enforcement authorities.⁷²

Unlike payment intermediaries, analytical bodies do not usually have comprehensive operational transaction systems at their disposal but rely instead on structured reporting data and institutional cooperation. Their effectiveness therefore depends largely on the quality, completeness and standardisation of the information received. At the same time, by aggregating reports from different parties subject to the reporting obligation, they can identify patterns that would not be apparent to individual intermediaries acting in isolation.

Financial transactions often represent only a small part of complex issues that encompass communicative, technical and international dimensions. This is relevant in the context of this study. Analytical assessments, through cross-sector analysis, can help to highlight links between cash flows, platform usage and international interdependencies, subject to statutory

⁷² Egmont Group (2023). Principles for Information Exchange Between Financial Intelligence Units, and: FATF (2023). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (FATF Recommendations)

powers and the legal framework governing data protection. Furthermore, international coordination networks play an important role in cross-border exchange of information. As digital financial flows often span several jurisdictions (see 3.2.3), structured cooperation mechanisms are required to prevent gaps in information. Standardised reporting formats, secure communication channels and harmonised typologies can enhance the comparability and efficiency of analytical processes.

The role of analytical and coordinating bodies is therefore neither purely operational nor purely normative. They operate at the interface between private risk identification and state law enforcement. Their position within the architecture is characterised by data aggregation, pattern analysis and institutional mediation. It is important to note, for the purposes of further analysis, that their effectiveness depends largely on the quality of cross-sector cooperation.

3.3.4 Law enforcement and investigative authorities

Law enforcement and investigative authorities play an independent role within the digital financial architecture, one that is anchored in criminal procedural law. Unlike payment intermediaries or analytical bodies, they do not operate primarily on a preventative or risk-based principle but rather based on specific grounds for suspicion within the framework of legally defined investigative powers. This group of stakeholders includes national police authorities, specialist units for combating cybercrime, public prosecutors' offices and international cooperation frameworks.

Their functional role consists of investigating matters relevant to criminal law, securing evidence and, where provided for by law, identifying and prosecuting suspects. Financial transaction data can serve as one investigative tool amongst many. It is typically analysed in conjunction with communication data, technical forensic findings and other evidence.

In the context of digital financial flows, law enforcement agencies regularly rely on information provided by other groups of stakeholders. Reports of suspected offences from analytical units, information provided by payment intermediaries and platform operators and requests for international legal assistance are key sources of information. The effectiveness of measures under criminal procedure therefore depends primarily on legally sound cooperation mechanisms and clearly defined structures of responsibility.

Transnational cases pose particular challenges for law enforcement. Digital financial flows may cross several jurisdictions, and platform infrastructure and the parties involved may be located in different countries. International cooperation mechanisms, joint investigation teams and standardised mutual legal assistance procedures are therefore of crucial importance in preventing gaps in information and ensuring that investigations are coordinated effectively.

The role of law enforcement agencies in cases of sexualised violence against minors in the digital sphere is characterised by a particular need for sensitivity. In addition to financial considerations, victim protection, the preservation of evidence in the digital environment and international cooperation are key areas of focus. Financial transactions can provide evidence about networks, communication relationships or monetisation structures, but this usually represents only part of a broader investigative picture.

From a systemic perspective, law enforcement and law enforcement authorities should therefore be viewed as part of a multi-tiered model of cooperation. They build on the preliminary work carried out by analytical units and on reports from institutions subject to reporting obligations but have independent investigative powers. A clear distinction between risk-based financial analysis and the presentation of evidence in criminal proceedings is of central importance for classification under the rule of law.

3.3.5 Regulatory and normative stakeholders

Regulatory and normative stakeholders establish the legal and regulatory framework within which digital financial and platform architectures operate. They shape the conditions governing identity verification, reporting requirements, data processing and institutional cooperation, thereby defining the structural parameters within which other groups of stakeholders operate. This group includes national supervisory authorities, supranational institutions and international standard-setting bodies.

At national level, financial supervisory authorities play a key role by overseeing financial institutions, payment service providers, e-money institutions and crypto-service providers, and by monitoring their compliance with anti-money laundering regulations. At European level, institutions such as the European Banking Authority (EBA), the newly established AMLA (the EU's Anti-Money-Laundering Authority) and the European Commission are involved in harmonising regulatory frameworks. International bodies – in particular the Financial Action Task Force (FATF) – develop global standards to combat money laundering and the financing of terrorism, which are transposed into national law by Member States.

In the digital context, specific regulatory frameworks for platforms and digital services are also becoming increasingly important. Regulations governing platform liability, transparency obligations and the risk assessment of digital services also indirectly influence the design of financial processes, particularly where payment functions form an integral part of the platform's architecture. This creates an interface between financial market regulation, digital regulation and criminal law.

The functional role of regulatory bodies is not to carry out transactions or investigations at an operational level, but to define minimum standards, risk categories and supervisory tools. They specify which institutions are subject to specific requirements, which due diligence obligations must be met and how the flow of information between private and public bodies must be organised. In this way, they influence the institutional architecture described in the preceding sections.

With regard to sexualised violence against minors in the digital sphere, this normative level creates the structural conditions necessary for prevention and detection mechanisms. Risk-based approaches, guidelines on transaction monitoring and requirements for international co-operation can have a significant impact on the scope for action of other groups of stakeholders. At the same time, regulatory measures must be consistent with data protection and fundamental rights safeguards in order to ensure proportionality and the rule of law.

Regulatory and normative bodies thus provide the framework within which payment intermediaries, platform operators, analytical bodies and law enforcement agencies operate. Their role helps to shape the structure and define the system, without direct involvement in individual transaction processes.

At the same time, the analysis makes it clear that no single stakeholder can fully grasp the overall picture of financial activities. Figure 5 illustrates the institutional visibility of data throughout the digital interaction and payment structures. Payment intermediaries have access to structured transaction data, platform operators to contextual interaction information, analytical bodies to aggregated risk assessments, and law enforcement agencies to powers of investigation under criminal procedure. Regulatory bodies also define the legal framework within which this information can be collected, processed and exchanged.

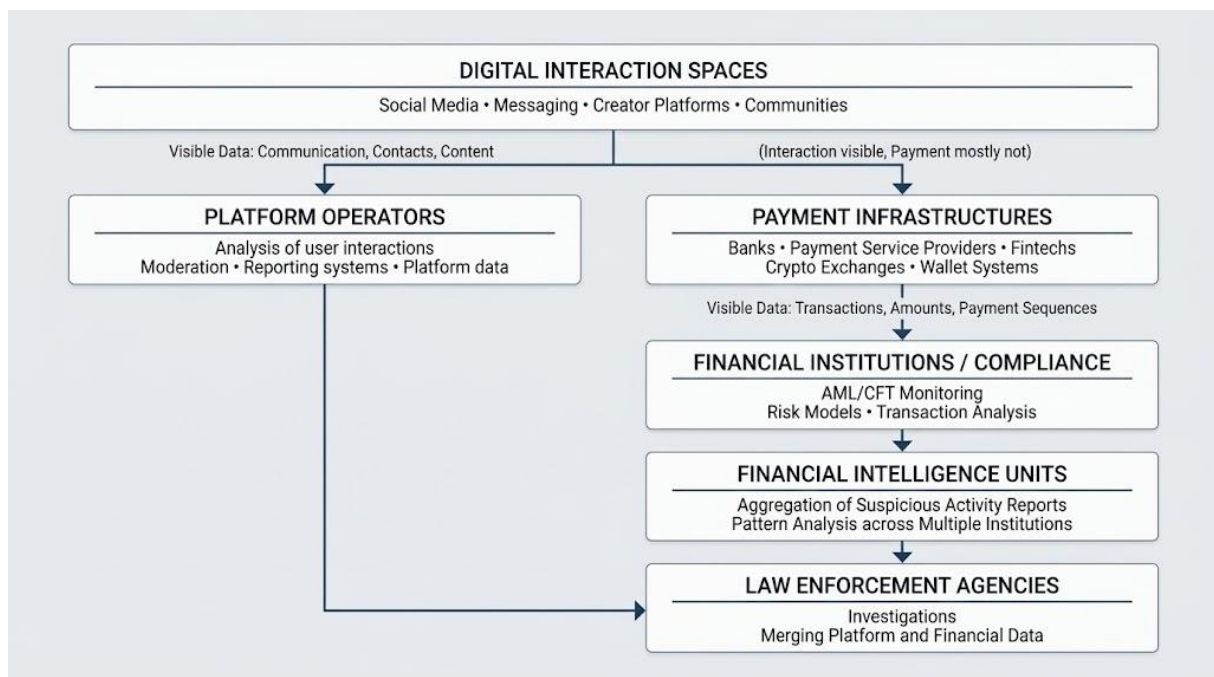


Figure 4: Visibility of relevant data

It follows from this architecture, which is based on the division of labour, that financial risks in the digital sphere can rarely be attributed solely to individual transactions. Relevant insights often only emerge when different sources of information and institutional perspectives are brought together. A systematic examination of recurring structures and scenarios is therefore necessary to analyse the interplay between digital interaction spaces, monetary mechanisms and institutional responsibilities.

Against this background, the following section focuses on the identification and systematisation of finance-related risk patterns. The aim is to describe, at an abstract level, typical structural features and recurring patterns which may be significant in conjunction with existing institutional mechanisms. The aim here is not to describe specific circumvention strategies or operational weaknesses, but rather to provide an analytical classification of patterns that may be relevant in the context of regulatory, analytical and preventive measures.

Section 3.4 thus builds on the payment mechanisms, systemic dynamics and roles of stakeholders outlined previously and develops a structured typology of finance-related indicators and red flags that can be observed or assessed in existing institutional structures.

3.4 Typologies and red flags

The preceding sections have outlined the infrastructural foundations of digital payment mechanisms (3.1), their economic and technical dynamics (3.2) and the roles of the institutional stakeholders involved (3.3). Building on these structural perspectives, the focus now turns to identifying recurring patterns in which financial transactions may occur in the digital space. The aim of this chapter is to systematise typical patterns and structural features that may be of analytical relevance in the context of sexualised violence against minors in the digital environment.

In international research and practice, the approach of typological analysis has become established in this context. Typologies serve to describe complex phenomena through abstracted patterns, without going into the details of individual cases. They make it possible to identify structural similarities across various individual cases and to organise them analytically. International organisations such as the Financial Action Task Force (FATF), Europol and national Financial Intelligence Units regularly use typological analyses to monitor developments in the field of financial crime and to support institutional risk assessments.

The typologies presented in this chapter are based on a combination of various sources: international research and analysis reports, publicly available studies on digital crime and online risks and the expert interviews conducted as part of this study with representatives from the financial sector, law enforcement, technology companies and civil society organisations. The aim is to highlight recurring structural features of digital financial flows and to assess their significance for institutional prevention and detection mechanisms.

It should be expressly emphasised that the following analysis does not describe operational strategies employed by perpetrators, technical vulnerabilities or methods of circumvention. Rather, the focus is on structural patterns, economic incentive mechanisms and the technological framework of digital financial systems. These are presented at a level of analytical abstraction that allows for scientific classification without revealing specific operational details.

In this context, four analytical perspectives are distinguished below. First, we examine typical payment and transaction patterns in digital financial flows (3.4.1). The basic forms of monetisation of digital interactions are then analysed (3.4.2). Building on this, the structural characteristics of digital network and platform architectures are discussed (3.4.3). Finally, institutional monitoring points and potential red flags that may be relevant within the framework of existing regulatory and analytical systems are summarised (3.4.4).

This structured typology is intended to create an analytical framework that clarifies the interplay between financial mechanisms, digital spaces for interaction and institutional responsibilities, thereby providing a basis for subsequent discussion of approaches to prevention, detection and cooperation.

A detailed table and list of typologies and red flags is available from ECPAT on request.

3.4.1 Payment and transaction patterns

Digital payment infrastructures enable a wide variety of different transaction types, some of which differ significantly in structure from traditional bank-based payment processes. In the context of sexualised violence against minors in the digital sphere, international studies and analytical reports reveal recurring patterns that are characterised not so much by individual transactions as by their sequence, frequency and embedding within digital interaction structures. The following observations describe the structural characteristics of such payment flows, without detailing the specific operational arrangements in individual cases.

A structural feature of digital financial flows that is frequently described is the fragmentation of payments into numerous smaller transactions. International analyses suggest that digital payment systems – in particular peer-to-peer transfers, platform-integrated payment functions and cryptocurrencies – make it easier, both technically and economically, to process very small amounts. This can give rise to payment flows whose economic significance stems from the sum of many individual transactions, while individual transfers, when viewed in isolation, are of small volume. Studies of digital financial crime suggest that such micro-transaction structures can occur in various forms of digital online economies, as they are associated with low barriers to entry and a high degree of repeatability.⁷³

Another recurring pattern involves regular or sequential payments that may extend over a longer period of time. Digital platform economies are often characterised by recurring financial transactions, such as subscription models, platform-based memberships and other forms of ongoing monetisation of digital content. International analyses of contexts of online exploitation show that monetary interactions can sometimes be embedded in such recurring structures, in which payments do not occur as isolated events but as part of ongoing interaction relationships.⁷⁴

Furthermore, cross-border transaction structures may arise, as digital payment infrastructures are not necessarily linked to national financial systems. International organisations point out that digital financial flows can often span several jurisdictions, particularly when platform providers, payment service providers and users are based in different countries. Such transnational structures are a general feature of digital markets and present analytical challenges for institutional actors, particularly regarding issues of jurisdiction and international co-operation.⁷⁵

In some cases, a combination of different payment methods can be observed. Digital ecosystems make it possible to link traditional fiat payment methods, internal platform payment systems and crypto-based transactions. International studies of the economics of online crime

⁷³ FATF (2025). Detecting, Disrupting and Investigating Online Child Sexual Exploitation

⁷⁴ Thorn (2024). Trends in Financially Motivated Sexual Extortion

⁷⁵ Europol (2025). Internet Organised Crime Threat Assessment (IOCTA)

suggest that hybrid payment structures may arise, in which different payment systems are combined within a digital interaction context. Such structures may arise for technological, economic or platform-related reasons and are not limited to specific criminal contexts.⁷⁶

Finally, international analyses suggest that financial transactions in the digital sphere are often closely linked to communication- or platform-based interaction structures. Payments may be directly linked to digital interactions, for example in connection with the provision of content, access to digital services or other forms of monetised interaction. This interlinking of interaction and financial flows is a fundamental characteristic of digital platform economies and influences the way in which monetary activities can be analysed.⁷⁷

The patterns described can be summarised analytically into the following typologies:

Fragmented microtransactions	→ breaking down monetary transactions into a large number of small individual payments
	→ economic significance arises from the cumulative total of many transactions
Sequential or recurring payments	→ regular financial transactions over an extended period
	→ partly embedded in digital interaction relationships
Cross-border microtransactions	→ transactions between different jurisdictions
	→ use of globally available digital payment infrastructures
Hybrid payment structures	→ a combination of various payment instruments, such as fiat payments, internal platform payment systems or crypto-based transfers
Platform-specific payment flows	→ monetary transactions directly linked to digital interactions or platform functions

The patterns described should be understood as structural typologies of digital financial flows. They set out recurring characteristics of digital payment systems and platform economies without breaking them down into specific individual cases. For institutional stakeholders, however, such structural observations may still be relevant, as they provide insights into the contexts in which financial activities may occur in digital interaction spaces and the areas where it may be worthwhile focusing analytical attention.

3.4.2 Monetisation models for digital exploitation

Digital communication and platform economies have created new opportunities to monetise interactions, content and digital services. These developments are not, in principle, confined

⁷⁶ UNODC (2024). Global Report on Trafficking in Persons

⁷⁷ BIS (2019). Big Tech in Finance: Opportunities and Risks

to criminal contexts, but characterise numerous legitimate business models in digital markets. Nevertheless, international studies show that certain monetisation mechanisms can also occur in contexts of sexualised violence against minors, particularly where digital spaces for interaction are linked to payment infrastructures. The following analysis describes the structural forms of such monetisation models at an abstract level.

A frequently described structural feature is models with payment-based access to digital content or interactive spaces. Digital platforms generally make it possible to link access to certain content or communication channels to financial transactions. International research into forms of online exploitation shows that financial transactions may, in some cases, be linked to such access arrangements in connection with exclusive content, for example, or closed digital groups.⁷⁸ In such cases, financial transactions act as a prerequisite for access to certain digital spaces for interaction.

Analyses of so-called "live distance child sexual abuse" – livestreaming of sexual exploitation – show that these offences are often facilitated by direct or indirect financial transactions between the perpetrators who commission the acts and the individuals carrying them out in person. In such cases, the perpetrators make payments to intermediaries, family members or other individuals involved who induce or coerce minors into performing sexual acts on themselves or on other minors. A characteristic feature of this type of offence is that the perpetrators who pay often not only finance commission of the acts themselves but also give specific instructions – both beforehand and during the live stream – regarding the nature, sequence and intensity of the sexual acts. The financial transaction serves as direct remuneration for the sexual exploitation and is a key factor in facilitating the offence. Analyses indicate that financial incentives, digital communication channels and real-time interaction are closely interlinked in these contexts.⁷⁹

Another pattern concerns platform-based monetisation mechanisms that were originally developed for legitimate digital business models. Platform economies often incorporate features such as subscriptions, virtual goods, digital gifts and other forms of micro-payment systems. International analyses of digital platform markets show that such monetisation tools can, in principle, be used in a variety of digital contexts, as they enable a direct link between interaction and financial transactions.⁸⁰

In addition, hybrid payment models may arise in which various payment instruments are combined. Digital ecosystems make it possible to link traditional fiat payments, internal platform credit systems and crypto-based transactions. International studies on the economics of online crime suggest that such hybrid structures can emerge in digital markets, as they link different technological and institutional infrastructures.⁸¹

Finally, international analyses show that monetary activities in the digital sphere are often embedded in network-like structures of interaction. Digital platforms enable the formation of communities, communication groups or distributed networks within which monetary transactions

⁷⁸ ECPAT International (2020). Summary Paper on Online Child Sexual Exploitation

⁷⁹ International Justice Mission (2020). Online Sexual Exploitation of Children in the Philippines

⁸⁰ Rochet, J.-C., & Tirole, J. (2003). Platform Competition in Two-Sided Markets, *Journal of the European Economic Association*, Volume 1, Issue 4, 1 June 2003, pages 990–1029

⁸¹ FATF (2025). Detecting, Disrupting and Investigating Online Child Sexual Exploitation

can take place. In such contexts, financial flows often do not arise as isolated individual transactions but as part of recurring interactions within digital communities.⁸²

The patterns described can be summarised analytically into the following typologies:

Access-based monetisation	→ payments as a prerequisite for access to digital content or interactive spaces, such as closed groups or exclusive digital content
Monetised real-time interactions	→ financial transactions arising from digital interactions between people who are physically separated, sometimes in conjunction with live communication or direct forms of interaction
Platform-based monetisation mechanisms	→ use of internal platform payment functions such as subscriptions, virtual goods or micro-payment systems
Hybrid payment models	→ the combination of several payment infrastructures, such as internal platform systems, fiat payments and crypto-based transfers
Network-based monetisation	→ monetary interactions within digital communities or communication networks, often organised as recurring transactional relationships

The monetisation models presented here should be understood as analytical typologies that describe the structural characteristics of digital interaction and payment economies. They illustrate how financial transactions can be embedded within digital communication and platform structures. For institutional stakeholders, such structural characteristics may be relevant in understanding the economic incentive mechanisms that can arise in digital spaces for interaction.

3.4.3 Network and platform structures

Digital interactions are increasingly taking place within complex platform and network architectures. Communication platforms, social networks, messaging services and specialised online communities form key infrastructures in which content, interactions and financial activities can be interlinked. These platform infrastructures are a defining feature of the digital economy and shape the structural conditions under which financial transactions also take place.

A key feature of digital platforms is their network-based organisational form. Platform economies connect different user groups – such as providers and consumers of digital content – within a shared technical system. Economic analyses show that such platforms are characterised by network effects: the value of a platform can go up as the number of users grows, since

⁸² Europol (2025). Internet Organised Crime Threat Assessment (IOCTA)

interactions, information flows and economic activity increase.⁸³ This network structure also influences the organisation of monetary interactions. Financial transactions on digital platforms can be closely linked to communication and interaction relationships. Payments may, for example, arise in connection with digital content, services or interactive formats facilitated within a platform. Platform operators can provide their own monetisation tools for this purpose or integrate external payment service providers (see 3.1.5).

International analyses of the economics of online crime suggest that such platform and network structures may also play a role in contexts of digital exploitation. It is not the platform technology itself that matters, but rather the ability to organise digital communication spaces and link financial transactions to interactions.⁸⁴ The resulting structures can take various forms, such as centralised platform models or more decentralised network structures:

→ In centralised platform structures, a platform operator acts as the organisational and technical hub of a digital interaction space. Content, user accounts and monetisation features are managed within a shared infrastructure. In such scenarios, communication and payment data can be combined within the same system, provided that the legal framework permits this.

→ In contrast, more decentralised network structures may arise, in which interactions are spread across several digital services. Communication channels, hosting infrastructures and payment mechanisms may be organisationally separate from one another. International analyses of the economics of digital criminal economies show that such decentralised structures can generally occur in many online contexts, as digital services can be combined in a modular way.⁸⁵

Regardless of the specific form it takes, the integration of communication and financial structures is a key feature of digital platform economies. Interactions, content and financial processes can take place within shared technical infrastructures or be interconnected in various ways via services. For institutional stakeholders, this presents the challenge of not viewing financial activities in isolation but rather analysing them in the context of digital interaction spaces.

The patterns described can be summarised analytically into the following typologies:

Centralised platform structures	→ digital interactions are organised within a single platform
	→ a platform operator manages the technical infrastructure, user accounts and monetisation functions
Decentralised network structures	→ use of multiple digital services for communication, content and payment processing
	→ organisational separation of the platform, hosting and payment infrastructure

⁸³ Rochet, J.-C., & Tirole, J. (2003). Platform Competition in Two-Sided Markets, *Journal of the European Economic Association*, Volume 1, Issue 4, 1 June 2003, pages 990–1029

⁸⁴ Europol (2025). Internet Organised Crime Threat Assessment (IOCTA)

⁸⁵ UNODC (2024). Global Report on Trafficking in Persons

Cross-platform interaction networks	→ digital interactions span multiple platforms or services
	→ different infrastructures each perform some of the functions
Community-based network structures	→ monetary interactions are embedded in digital communities
	→ recurring interactions between members of digital networks
Hybridised communication and payment networks	→ a combination of different platform and payment infrastructures within a single interaction context

An analysis of network and platform structures thus illustrates that financial transactions in the digital space are often part of complex systems of interaction. When analysing financial risks, therefore, it is not only the individual transaction that is relevant but also the way in which monetary activities are embedded in digital communication and platform architectures.

3.4.4 Institutional red flags and monitoring points

The payment and transaction patterns, monetisation mechanisms and network structures described above may be of analytical relevance to institutional stakeholders when they occur in certain constellations. In international financial supervision, within Financial Intelligence Units and in law enforcement, such recurring structural features are often referred to as red flags or observation points. They do not constitute evidence of criminal behaviour, but rather indications of circumstances which may require further analysis or institutional attention.

International organisations such as the Financial Action Task Force (FATF), Europol and national financial intelligence units use red-flag approaches as part of their risk-based analysis procedures. The aim is to identify patterns which, when combined with other information, may indicate potentially risk-related activities. Red flags are therefore not stand-alone criteria but are regularly assessed as part of extensive risk analyses.⁸⁶

In the context of digital platform economies, red flags can arise both from financial transaction patterns and from the structure of digital interaction spaces. The dynamics of digital markets described above – especially the fragmentation of transactions, scaling of digital interactions, transnational infrastructure and integration of communication and payment data – may influence the way in which such observation points are analysed (see 3.2). This presents financial intermediaries and analytical bodies with the challenge of not viewing financial activities in isolation but rather analysing them in the context of digital platform and network structures.

Another important aspect relates to the institutional perspective on such indicators. Different groups of stakeholders have different access to information and opportunities for observation.

⁸⁶ FATF (2025). Detecting, Disrupting and Investigating Online Child Sexual Exploitation

Payment intermediaries can analyse transaction data; platform operators have access to contextual information from digital interaction spaces; and analytical bodies can identify structural patterns by aggregating various reports. The assessment of potential risk scenarios is therefore often carried out through collaboration between several institutions.⁸⁷

International studies of combating digital financial crime also emphasise that red flags in a digital context are often pattern-based rather than exclusively transaction-based. Whereas traditional financial analysis often focuses on individual transactions, sequences of transactions, recurring patterns of interaction and network structures are becoming increasingly important in the digital sphere.⁸⁸ Analytical assessment of such patterns typically takes place as part of risk-based compliance and analysis procedures.

The red flags summarised below should therefore be understood as institutional observation points that may arise in various contexts. They describe structural patterns in digital financial and interaction systems and serve to provide an analytical framework for classifying potential risk scenarios. They are always assessed in the context of further information and are subject to the relevant legal and regulatory framework conditions.

Based on international analyses, the following categories of institutional observation points can be distinguished:

Financial structural indicators	→ unusual patterns of many small transactions occurring within short periods
	→ recurring monetary transfers between the same digital stakeholders
	→ transaction structures involving highly fragmented payment amounts
	→ repeated cross-border microtransactions
	→ combination of various payment methods within the same interaction context
Platform- and interaction-related indicators	→ monetised interactions within digital communication spaces
	→ linking of digital interaction events and financial transactions
	→ use of closed digital groups or communities with monetary access elements
	→ recurring monetary activities within digital interaction networks
Network-related structural indicators	→ highly centralised payment flows to individual accounts or wallet addresses
	→ cluster-like payment relationships within digital networks
	→ recurring monetary interactions within stable digital communities

⁸⁷ Europol (2025). Internet Organised Crime Threat Assessment (IOCTA)

⁸⁸ Egmont Group (2025). Principles for Information Exchange between Financial Intelligence Units

Institutional observation points	→ cross-platform interaction and payment structures
	→ interfaces between platform infrastructure and payment service providers
	→ on- and off-ramp structures between crypto-based and traditional payment systems
	→ recurring reports of suspicions about similar structural patterns from different institutions
	→ cross-border interaction and payment structures involving several jurisdictions

3.5 Comparison: Global vs. DACH-specific patterns

The typologies of financial structures and monetary interaction patterns in the digital space outlined above are based primarily on international studies, global analytical reports and cross-sector experiences of financial institutions, law enforcement agencies and technology companies. Digital communication platforms, payment infrastructures and crypto-based transaction systems are fundamentally global in scope in terms of their technical functioning. Interactions, content and financial transactions can therefore take place across national borders and are often embedded in transnational network structures.

At the same time, the institutional framework for combating cybercrime is predominantly organised at national level. Regulatory frameworks, the remit of supervisory and law enforcement authorities and institutional cooperation structures vary, in some cases significantly, between individual countries and jurisdictions. These differences may influence how financial risks are identified, assessed and addressed.

Against this background, it is useful to compare the global structural patterns outlined above with the institutional and regulatory frameworks in the German-speaking world – specifically in Germany, Austria and Switzerland (DACH). The aim of this section is not to develop new typologies, but to place international observations in the context of the regional financial and supervisory architecture.

The comparison focuses on three key dimensions: firstly, the globally observable structural patterns of digital financial flows; secondly, the institutional and regulatory characteristics of the DACH region; and thirdly, the role of the financial sector and inter-institutional cooperation in identifying and assessing potential risk scenarios. The aim of this classification is to highlight the areas in which global developments are also relevant in a regional context and where institutional particularities may affect the practical implementation of prevention and detection measures.

3.5.1 Global structural patterns of digital financial flows

International studies into the economics of digital crime show that financial transactions in the digital space often follow specific structural patterns that are comparable across different regions. These patterns are shaped less by national characteristics than by the technical and economic characteristics of digital platform economies and globally available payment infrastructures. Digital communication platforms, online marketplaces and crypto-based payment systems create spaces for interaction in which financial activities can generally be organised across borders.

The international literature identifies the following recurring structural features of digital financial flows:

- **Fragmented microtransactions:** numerous smaller transactions of cumulative economic significance;
- **Platform-based payment structures:** monetisation of digital interactions within platform economies;
- **Transnational payment networks:** cross-border interaction and payment structures;
- **Hybridised payment infrastructures:** a combination of different payment methods (fiat, platform payments, cryptocurrencies);
- **Network-based financial structures:** financial transactions embedded in digital communication and interaction networks.

These global structural patterns form the basis for the following comparison with the institutional frameworks and specific characteristics in German-speaking countries.

3.5.2 Institutional and regulatory characteristics in the DACH region

In German-speaking countries – in particular Germany, Austria and Switzerland – the fight against financial criminality is heavily influenced by the respective financial market regimes, supervisory structures and international cooperation.

Regulation around anti-money laundering (AML) plays a key role in this regard. International standards set by the Financial Action Task Force (FATF) require countries to implement risk-based approaches to combating money laundering and the financing of terrorism. These standards have been implemented in the European Union, specifically through the European Anti-Money Laundering Directives and the corresponding national legislation. Financial institutions and payment service providers are therefore required to operate risk management systems, analyse suspicious activities and, where necessary, submit reports to the relevant Financial Intelligence Units.⁸⁹

⁸⁹ FATF (2025). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation

The European Anti-Money Laundering Directives (AMLD) form the key regulatory framework for combating money laundering and terrorist financing within the European Union.⁹⁰ They require Member States to transpose certain minimum standards into national law, in particular with regard to the due diligence obligations of financial institutions, the establishment of national financial intelligence units and the reporting of suspicious transactions. The Directives thus define fundamental structural elements of the European AML system, including in particular:

- obligations for "obliged entities" such as banks, payment service providers and other financial intermediaries;
- establishment of national Financial Intelligence Units (FIUs) as central analysis and reporting centres;
- mechanisms for reporting suspicious transactions;
- requirements relating to risk assessments, supervision and international cooperation.

At the same time, the AML Directives are harmonisation instruments that set minimum standards. The specific institutional arrangements – such as the organisational integration of the FIU, the structure of financial supervision and operational cooperation between authorities and the financial sector – are left to the individual Member States to determine. This results in different institutional models for combating money laundering within the European Union, even though the fundamental regulatory principles are largely harmonised. With the establishment of a European Authority for Combating Money Laundering and Terrorist Financing (AMLA), in conjunction with the 6th Money Laundering Regulation, the EU is seeking to establish a so-called single rulebook.⁹¹

In the DACH region, the institutional structure for combating money laundering is structured in accordance with EU requirements. Institutions such as the Federal Financial Supervisory Authority (BaFin), the Austrian Financial Market Authority (FMA) and the Swiss Financial Market Supervisory Authority (FINMA) monitor financial institutions' and payment service providers' compliance with anti-money laundering obligations.⁹² These supervisory structures help to ensure that risk management and compliance systems are systematically implemented in the financial sector.

This establishes a system of division of labour between the financial sector, supervisory authorities and Financial Intelligence Units. Financial institutions play a key role in identifying potentially suspicious transactions as part of their compliance and monitoring systems. Reports of suspected offences are then forwarded to the relevant Financial Intelligence Units, which carry out a more detailed analysis and, where necessary, involve the investigating authorities. The multi-tiered structure of this governance architecture is illustrated in Figure 5.

Another characteristic of the DACH region is the increasing level of institutionalised cooperation between public- and private-sector stakeholders. In recent years, public-private

⁹⁰ EU (2024). Directive (EU) 2024/1640

⁹¹ EU (2024), Directive (EU) 2024/1620

⁹² See BaFin (2025) Auslegungs- und Anwendungshinweise zum Geldwäschegesetz (AuA AT), FMA (2024) Financial Markets Anti-Money Laundering Act (Consolidated Version), FINMA (2023), Ordinance of the Swiss Financial Market Supervisory Authority on Combating Money Laundering and Terrorist Financing in the Financial Sector (GwV-FINMA)

partnership models have been developed in various European countries to improve the exchange of information between financial institutions, public authorities and other relevant stakeholders. Such forms of cooperation can help to identify structural patterns in financial activities more effectively and to build up joint analytical capabilities.⁹³

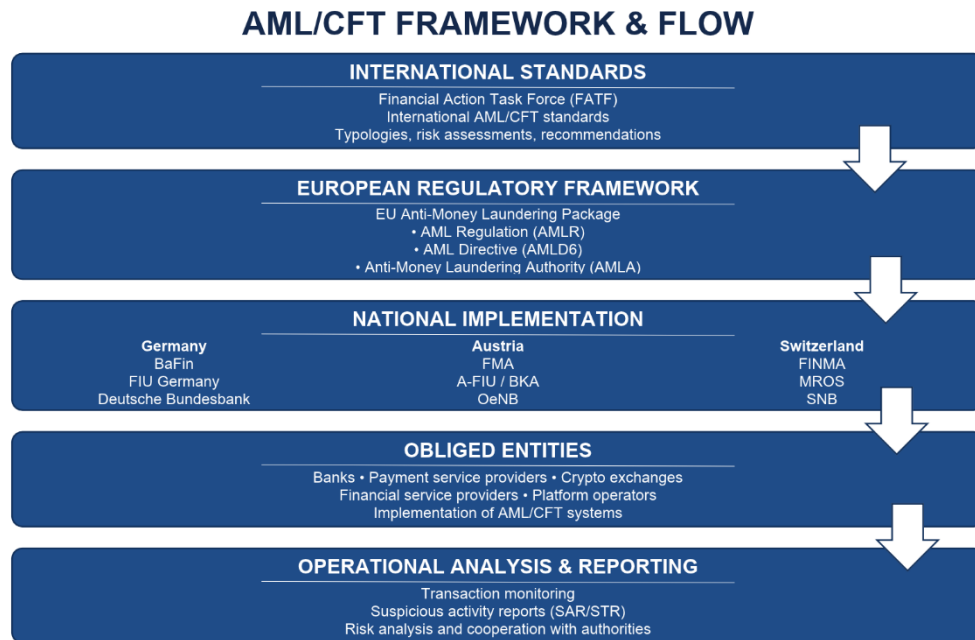


Figure 5: International standards & national implementation

Furthermore, European regulation of digital markets is increasingly shaping the institutional framework. Initiatives such as the Digital Services Act (DSA) and regulatory measures relating to digital platforms aim to strengthen platform operators' responsibility for content, interactions and risk management. In the long term, these developments may also have an impact on co-operation between platform operators, financial intermediaries and law enforcement agencies.⁹⁴

Overall, it is evident that the DACH region is characterised by a relatively well-developed regulatory framework in the areas of financial market supervision and anti-money laundering. These institutional frameworks have a significant influence on how global structural patterns in digital financial flows are identified, assessed and addressed in practice.

3.5.3 The financial sector and institutional cooperation in the DACH region

The financial sector plays a key role in the fight against money laundering, terrorist financing and related forms of digital crime. Banks, payment service providers, fintech companies and

⁹³ Europol (2023). EFIPPP Practical Guide for Operational Cooperation between Investigative Authorities and Financial Institutions

⁹⁴ EU (2022). Regulation (EU) 2022/2065

providers of crypto-based financial services are required to implement risk-based measures to prevent, identify and report potentially suspicious activities. These obligations arise from the international standards of the Financial Action Task Force (FATF), from European legislation around anti-money laundering and from the national legal provisions of the respective countries.⁹⁵

A key part of this responsibility is the implementation of transaction monitoring and risk management systems, which can be used to identify unusual or potentially risky financial transactions. Financial institutions analyse transaction data, customer profiles and other risk factors in this context in order to identify any potential anomalies and, where necessary, submit suspicious activity reports to the relevant Financial Intelligence Units.⁹⁶ These reports represent a key channel of information through which financial institutions help to uncover potential criminal activity.

In the DACH region, cooperation between financial institutions and government bodies has become increasingly institutionalised in recent years. In addition to statutory reporting obligations, cooperative arrangements between the financial sector, supervisory authorities and law enforcement agencies have developed in many countries. Such collaborations may, for example, involve sharing risk indicators, typological findings or general situation assessments. International organisations such as Europol and the FATF emphasise the importance of such public-private partnership models in enabling a better analysis of complex financial structures in the digital sphere.⁹⁷

Furthermore, collaboration with technology companies and platform operators is becoming increasingly important. Digital interactions, platform economies and payment infrastructures are often closely interlinked. In many cases, platform operators have information about communication and interaction patterns, while financial intermediaries have transaction data. Coordinated collaboration can therefore help to bring together different data perspectives and provide a more comprehensive picture of digital financial structures.⁹⁸

At the same time, experience shows that institutional cooperation in the digital context can present various challenges. Differences in legal frameworks, data protection requirements and organisational responsibilities can affect the exchange of information between institutions. The international dimension of digital platform and payment structures also often requires cooperation across national borders. Against this background, further development of international cooperation mechanisms is becoming increasingly important.

Overall, the analysis highlights that the financial sector in the DACH region plays a key role in identifying potential risk scenarios. At the same time, effective prevention and analysis mechanisms are increasingly reliant on coordinated cooperation between financial institutions, platform operators, supervisory authorities and law enforcement agencies.

⁹⁵ FATF (2023). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation

⁹⁶ BaFin (2024), Auslegungs- und Anwendungshinweise zum Geldwäschegesetz

⁹⁷ Europol (2023). EFIPPP Practical Guide for Operational Cooperation between Investigative Authorities and Financial Institutions

⁹⁸ BIS (2019). Big Tech in Finance: Opportunities and Risks

The role of the financial sector and institutional cooperation in the DACH region can be summarised in terms of several key structural features:

- **Key role of obliged entities:** banks, payment service providers and financial intermediaries as the first line of defence against potentially suspicious transactions
- **Transaction monitoring and risk assessment:** use of risk-based compliance and analysis procedures to identify unusual transaction patterns
- **Suspicious activity reporting as a central information interface:** submission of reports to Financial Intelligence Units
- **Public-private partnership models:** cooperation between the financial sector, supervisory authorities and investigation bodies
- **Increasing cooperation with technology and platform companies:** integration of different data perspectives from interaction and financial systems
- **International cooperation mechanisms:** cooperation between national authorities and international organisations to analyse cross-border financial structures

These institutional cooperation mechanisms form a key basis for the analysis and assessment of financial activities in the digital sphere.

The institutional classification and handling of such structures depend heavily on regional regulatory and organisational frameworks. While the technical foundations of digital interactions are comparable across the globe, supervisory systems, jurisdictional structures and cooperation mechanisms differ, in some cases significantly, between individual states and legal jurisdictions. For example, international analyses distinguish between various institutional models of Financial Intelligence Units (FIUs), which differ particularly in terms of their organisational integration and their proximity to law enforcement agencies.⁹⁹ A distinction is often made between administrative, law enforcement-related and hybrid organisational forms. While administrative FIUs primarily carry out analytical functions and pass on their findings to investigative authorities, law enforcement-orientated FIUs are more closely integrated, from an organisational perspective, into police or investigation-related structures. Table 2 provides an overview of selected institutional models.

Country / Jurisdiction	Institution	Organisational integration	Type of FIU model	Distinctive features
Germany	FIU Germany	General Customs Directorate / Federal Ministry of Finance	Administrative FIU model	Focus on the analysis of suspicious transaction reports (STR/SAR), referral to law enforcement agencies
Austria	A-FIU (Federal Criminal Police Office)	Federal Criminal Police Office / Ministry of the Interior	Law enforcement FIU	Integration into police structures, close links with investigative authorities
Switzerland	MROS	Federal Office of Police (fedpol)	Administrative FIU model	Analysis of reports and referral to law enforcement agencies

⁹⁹ IMF (2004). Financial Intelligence Units – An Overview

USA	FinCEN	US Department of the Treasury	Law enforcement-oriented / hybrid model	Close operational cooperation with investigative authorities, comprehensive data collection
Singapore	MAS	Monetary Authority of Singapore	Hybrid / regulatory model	Combination of financial supervision, analysis and international cooperation

Table 2: Comparison of institutional models of selected FIUs

The comparison between global structural patterns and regional institutional frameworks thus highlights a fundamental tension between global digital markets and nationally organised regulatory and supervisory systems. Digital platform economies and payment infrastructures often operate across national borders, while responsibilities for supervision, law enforcement and regulation are predominantly organised at national level. This structural landscape poses a key challenge for the analysis and combating of digital financial crime and increasingly calls for coordinated international cooperation mechanisms.

Consequently, it becomes clear that an analysis of financial activities in the digital context must consider both global structural patterns and regional institutional frameworks. While global typologies provide insights into recurring patterns in digital interaction and payment structures, regional regulatory and institutional contexts play a decisive role in determining how such patterns can be identified, assessed and addressed.

This classification also forms the basis for the empirical analysis that follows. Section 4 draws on the structural patterns and institutional frameworks outlined above and examines how these are perceived and assessed in practice by financial institutions, regulatory authorities and other relevant stakeholders.

IV. Results of the empirical analysis

The preceding sections have outlined the structural foundations of digital interaction spaces, monetary mechanisms and institutional analytical processes. Building on this conceptual framework, the focus now turns to the empirical findings of the present study. The aim of this section is to bring together key findings from interviews with experts, secondary research sources and institutional analyses, and to contextualise them within the analytical framework developed previously.

The empirical analysis is based on a qualitative assessment of interviews with representatives from various institutional sectors, including financial institutions, payment service providers, blockchain analysis firms, law enforcement agencies, financial intelligence units, social organisations and international initiatives working to combat digital exploitation. These interviews were supplemented by a systematic review of international studies, analytical reports and institutional publications.

The study assumes that financial activities in the digital space do not typically occur in isolation, but are embedded within complex structures of interaction, platforms and payments. Digital communication, financial transactions and institutional analytical processes form a multi-tiered system in which different groups of stakeholders each adopt specific perspectives from which to observe the system. While platform operators are primarily able to collect interaction and usage data, financial institutions have access to transaction information, and government analysis and investigation bodies can combine various sources of information.

This multi-tiered structure of digital interaction and payment processes is illustrated in Figure 6, which summarises the analytical relationship between digital interaction spaces, monetary mechanisms and institutional analysis processes.

The aim of the empirical study is not to reconstruct individual case scenarios or to present operational investigation information. Rather, the aim is to identify structural patterns that can be observed from the perspective of various institutional stakeholders in connection with financial activities in the digital context. The analysis focuses on recurring transaction patterns, monetary incentive structures and the role of digital platform and network configurations. This empirical analysis is based on a triangulated evaluation of interviews with experts, international studies and analytical reports from relevant organisations.

In order to organise these observations systematically, the following presentation is based on two analytical perspectives. Firstly, the findings are categorised according to the 4Cs typology of digital risks (Content, Contact, Conduct, Commerce) introduced in Section 2. Secondly, the study examines financial risk structures that may arise from transaction patterns, platform dynamics and network structures.

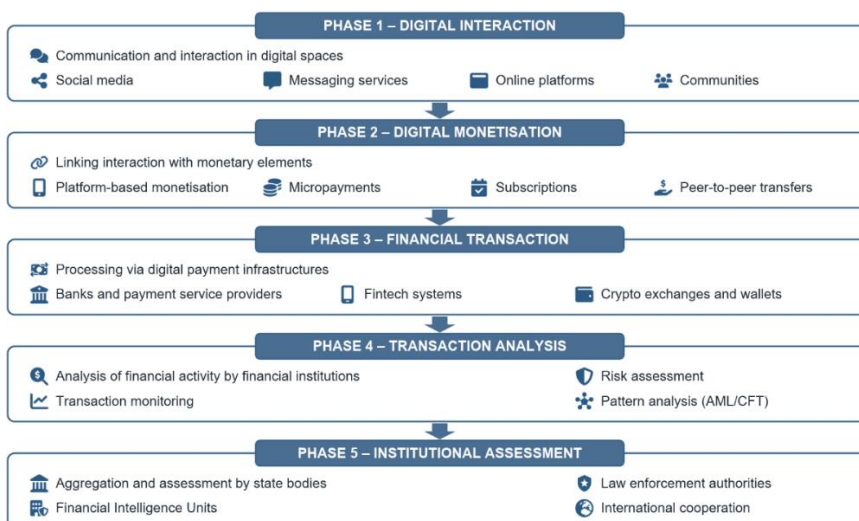


Figure 6: Digital interaction, monetisation and financial analysis

The empirical findings are presented step by step below. First, the observations are categorised structurally using the 4Cs model and the financial risk categories identified (4.1). Key patterns of digital financial interactions are then analysed, broken down by transaction structures, network dynamics and platform mechanisms (4.2). Building on this, the relationships between different payment forms, levels of anonymity and risk profiles are examined (4.3). Finally, the empirical findings are brought together in a consolidated typology of financial risk patterns (4.4).

4.1 Structural analysis using the 4Cs model and financial risk categories

The present study draws on the 4Cs model of digital risks (Content, Contact, Conduct, Commerce) introduced in Section 2.5 to structure the empirical analysis. The model serves as an analytical research framework for classifying different forms of digital interaction and risk structures in an online context. In this study, this model is used to categorise the findings from interviews and secondary sources according to key dimensions of interaction within digital platform ecosystems and to highlight their connection to forms of digital sexualised violence against and exploitation of minors.

While the categories Content, Contact and Conduct primarily describe communicative and social interaction structures, the category Commerce offers an analytical perspective on monetary activities in the digital space. This dimension is of particular significance for the present study, as it establishes a link between digital interaction spaces and financial transaction structures. This allows the analysis of digital dynamics of exploitation and violence to be expanded to include a financial perspective, which is particularly relevant for financial institutions, payment service providers and supervisory authorities.

This dimension is of particular significance for the present study, as it establishes a link between digital interaction spaces and financial transaction structures – thereby opening up an analytical approach that is specifically relevant to commercial forms of sexual exploitation of minors. This includes, in particular, monetised livestreaming of sexual exploitation, distribution of depictions of sexualised violence against children and young people in exchange for payment, financially motivated sexual extortion (FMSE) and hybrid forms such as so-called "pocket money dates".

On this basis, this study combines the 4Cs model with a complementary financial analysis of digital interaction and payment structures. The aim is to analyse the interplay between digital platform dynamics, monetary incentive structures and financial transaction patterns in a systematic way. In particular, the following levels of financial analysis are taken into account:

Transaction structures	→ such as sequences of microtransactions or recurring payment schedules
Monetisation models	→ for example, pay-per-view models, subscription schemes, package-based offers and peer-to-peer payments

Platform dynamics	→ in particular, the role of digital platforms in organising interactions and monetisation processes
Network structures	→ that is, relationships and patterns of interaction between participants within digital communities
Payment infrastructures	→ including account-based payment systems, peer-to-peer transfers and crypto-based payment methods
Identifiability of transactions	→ that is, the extent to which financial transactions can be traced at an institutional level and attributed to specific actors

The empirical evaluation of the interviews was carried out in two successive stages of analysis. Initially, the interviewees' statements were recorded in a structured interview matrix, in which the perspectives of various stakeholder groups – including financial institutions, payment service providers, blockchain analysis firms, law enforcement agencies, Financial Intelligence Units and social organisations – were documented according to standardised categories. This matrix serves as a documentation tool to enable a comparison of the diverse perspectives of the participating institutions and to record key observations systematically.

In a second step, the observations recorded in the interview matrix were analysed across all sources and consolidated into recurring structural patterns. On this basis, consolidated typologies of financial interaction and transaction structures were developed.

In the context of this study, a typology refers to a recurring pattern comprising interaction structure, platform context and financial transaction characteristics, as described in several interviews or sources. Typologies thus bring together different analytical dimensions – digital interactions, monetary structures and institutional perspectives – and enable a structured representation of complex phenomena.

This two-stage approach also serves an important purpose in terms of the confidentiality of the interviews. Several interviewees stipulated that their statements should not be quoted in a way that can be directly linked to their institutions. Through the structured transfer of interview content from the source level (interview matrix) to a consolidated typological level (typology matrix), individual statements are therefore not reproduced in isolation but are presented as part of overarching patterns.

The empirical findings are therefore not presented as descriptions of the individual positions of specific institutions, but as a synthesised analysis of recurring structural patterns derived from several sources. This approach makes it possible to analyse the insights provided in the interviews systematically while, at the same time, taking into account the interviewees' requests for anonymity.

4.2 Patterns identified

An analysis of the interviews and the secondary sources consulted reveals several recurring patterns in financial interactions in the digital space. These patterns should not be understood as isolated individual phenomena, but rather as recurring combinations of interaction structure, platform context and financial transaction characteristics. It is important to understand these in order to recognise their impact on the dynamics of sexualised violence and the exploitation of minors. By combining the insights from the interviews with existing analyses by international organisations, it was possible to identify several consolidated typologies describing different forms of monetised digital interactions.

The following sections present these patterns in three key analytical dimensions: transaction structures, network structures and platform dynamics. These dimensions form the basis for the typology of financial interaction structures developed subsequently.

4.2.1 Transaction structures

One of the key findings of the analysis concerns the structure of financial transactions. The interviews and studies analysed repeatedly described how monetary interactions in a digital context often do not take the form of individual payments, but rather of sequences of several transactions organised according to specific patterns in terms of timing and amount.

Several interviewees pointed out that microtransactions and fragmented payment sequences, in particular, can play a key role. Such transaction structures may, for example, consist of recurring small amounts transferred at short intervals or of several instalments. In some cases, package-based payment models or subscription-style structures were also described, whereby payments are made regularly or at specific intervals.

In addition to the fragmentation of payments, the use of a combination of different payment instruments was also described as a recurring pattern. For example, financial transactions may begin via traditional account-based payment systems and then continue using alternative payment methods or crypto-based transactions. This combination of different payment infrastructures can mean that individual transactions appear unremarkable when viewed in isolation, while a structured pattern only becomes apparent when viewed within the broader context of a transaction history.

Analysis of the interviews also shows that transactional patterns often manifest themselves in specific temporal dynamics. These include, for example, short-term series of transactions, periodic payment sequences and recurring payment patterns, which may be linked to specific platform activities. These observations are consistent with international analyses, which suggest that digital payment structures are increasingly characterised by highly fragmented and dynamic transaction patterns.

The transaction patterns described – especially fragmented micropayments and recurring sequential payment patterns – were mentioned explicitly by several interviewees in connection with the sexual exploitation of minors. They occur both in the context of commercial livestreaming exploitation, where payments may be directly linked to individual instances of

interaction, and in cases of FMSE, where a series of payments are organised under duress. These patterns are therefore not merely technical characteristics of digital payment systems, but reflect specific patterns of behaviour that can be empirically observed in connection with the sexual exploitation of minors.

4.2.2 Network structures

In addition to the transaction structures, the interviews described recurring network dynamics. Digital interactions and monetary transactions often take place within specific social or platform-based networks, in which stakeholders can assume different roles.

Several interviewees described how monetary interactions often do not take place between isolated individuals but are organised within loose network structures. These may, for example, consist of smaller groups, community structures or loosely connected interaction networks. Different roles may arise within such networks, including providers, intermediaries and consumers of digital content.

Another recurring pattern concerns the intermediary role played by individual platform users or community members, who can act as links between different networks. Such actors may, for example, pass on or coordinate content, contacts or payment details within a network. In a number of interviews, it was pointed out that these intermediary roles can play an important part in organising interactions within certain digital communities.

Such intermediary roles are identified in the context of the sexual exploitation of minors, as shown by international analyses: they are involved, for example, in acting as intermediaries between perpetrators and victims, in the distribution of depictions of sexualised violence within closed networks and in the coordination of livestreaming of sexual exploitation. Linking such network roles to financial transaction flows is particularly relevant from an analytical perspective, as payment relationships can provide insights into structures and hierarchies within a network that would not be apparent from communication data alone.

Furthermore, both interviews and international studies show that digital networks are often organised across different platforms. Interactions may, for example, begin on one platform, while communication, organisation or payment processing take place on other platforms or communication channels. These cross-platform structures can mean that individual institutions are only able to observe specific aspects of a larger network of interactions.

4.2.3 Platform dynamics

Another key finding concerns the role of digital platforms as structural frameworks for monetary interactions. It became clear in almost all the interviews that platform architectures and monetisation mechanisms can have a significant influence on the organisation of digital interactions.

Digital platforms not only facilitate communication and interaction between users, but also frequently provide integrated monetisation features. These include, for example, subscription-

based models, pay-per-view access, virtual goods and platform-based payment systems. Such structures can help to integrate monetary interactions directly into digital interaction spaces.

At the same time, it was pointed out in several interviews that monetary transactions do not necessarily have to take place within the platform itself. In many cases, platform interactions can be combined with external payment infrastructures. For example, an interaction may take place on a platform, while the actual payment is processed via external payment services or alternative payment systems.

This combination of platform interactions and external payment structures can result in digital monetisation processes being spread across several technical and organisational levels. While platform operators are primarily able to collect interaction and usage data, financial institutions have access to information about payment structures, and government analysis and investigation bodies can combine these different sources of information, at least to some extent.

The patterns described show that digital interaction and monetisation structures are characterised by a combination of transaction sequences, network dynamics and platform-based interaction spaces. The structural patterns outlined also form the basis for the typology of recurring financial interaction structures developed in due course. Against this background, the question arises as to what role different payment infrastructures and forms of payment play within these structures, and how this can give rise to different risk profiles.

The following section therefore examines the relationships between different payment methods, the degree to which transactions can be traced back to specific institutions and the structural patterns observed.

4.3 Links between payment methods, anonymity and risk profiles

Analysis of the interviews and the secondary sources consulted shows that different payment infrastructures not only exhibit technical differences but also vary in terms of their institutional observability and the identifiability of the actors involved. These differences have a significant impact on the extent to which financial transactions can be tracked and assessed by financial institutions, payment service providers and analytical authorities. These differences are of direct practical relevance to the present study: the less traceable a payment infrastructure is, the more difficult it is for the authorities to identify transactions that may be linked to the sexual exploitation of minors.

Digital payment infrastructures differ in terms of the scope for institutional traceability of transactions and the parties involved. Key factors in this regard include regulatory identity requirements, the structure of the relevant payment infrastructure and the availability of institutional data access. For analytical purposes, payment structures can therefore be examined in two dimensions:

1. identifiability of the parties involved
2. institutional observability of the transaction

On this basis, payment infrastructures can be classified into three categories for the sake of simplicity.

Category I – High identifiability and high institutional observability. Infrastructures in this category are characterised by clear regulatory identity requirements and institutional control mechanisms. Transactions can generally be attributed clearly to specific account holders, and financial institutions are subject to comprehensive monitoring and documentation requirements. Typical examples of this include:

- bank transfers (e.g. SEPA);
- account-based payment services;
- regulated electronic payment services.

Payment infrastructures in this category have the following characteristics:

- identity verification as part of KYC processes;
- transaction monitoring by financial institutions;
- option to report suspicious transactions;
- institutional data access for analytical authorities.

Category II – Moderate identifiability and limited institutional observability. This category covers payment structures in which either identification or institutional observability is restricted. While transactions are, in principle, traceable, they require additional analysis or contextual information. These typically include:

- peer-to-peer payment services;
- platform-integrated payment functions;
- regulated crypto exchanges (on/off-ramp structures).

The key features of this category are, in particular:

- user accounts or wallets used;
- limited access to contextual information;
- transaction data fragmented in part;
- reliance on cooperation between platforms and financial institutions.

Category III – Low identifiability and restricted institutional observability. In this category, there are restrictions to traceability by institutions. While technical traces may exist (e.g. public blockchain data), it is often difficult to link them directly to identifiable actors, or such a link may only be possible indirectly. Typical examples include:

- self-custody wallets;
- direct peer-to-peer transfers without regulated intermediaries;
- certain alternative payment methods.

Transactions falling into this category have the following characteristics *inter alia*:

- limited or absent link to identity;
- no direct institutional monitoring of transactions;

→ analysis is often only possible via network or pattern recognition.

Analysis of the interviews shows that account-based payment systems generally allow for a comparatively high level of identifiability. Traditional bank transfers and account-based payment services typically involve identity checks as part of regulatory Know Your Customer processes. Financial institutions therefore have structured information about account holders, transaction amounts and payment sequences. This data forms an important basis for transaction monitoring and risk-based analysis procedures in the context of anti-money laundering.

Category	Identifiability	Institutional observability	Examples of infrastructure
I	High	High	Bank transfers, account-based payment services
II	Moderate	Moderate	Peer-to-peer payment services, platform-based payments
III	Low	Restricted	Self-custody wallets, direct blockchain transfers

Table 3: Classification of digital payment infrastructures

By contrast, other forms of payment exhibit varying degrees of institutional observability. While peer-to-peer payment services and platform-based payment functions may also include account-based elements, they are often more deeply embedded in digital interaction platforms. In such scenarios, financial institutions have access to information about the transactions themselves, while contextual information regarding platform interactions or user relationships is only available to a limited extent. Several interviewees pointed out that it is precisely this separation of communication and transaction data that can pose a challenge when interpreting individual payment structures.

Another aspect concerns crypto-based payment structures. Blockchain-based transactions are technically transparent and, in many cases, can be traced at network level. At the same time, it is often only possible to link such transactions to identifiable parties indirectly, for example via regulated interfaces such as cryptocurrency exchanges or other service providers. In practice, this results in a situation in which, while transaction flows can be analysed, the institutional traceability of the parties involved varies.

The interviews also show that monetary interactions in a digital context often combine several payment infrastructures. Interactions may, for example, be organised via platform-based communication channels, while the actual payment is made via external payment services or crypto-based systems. Such hybrid payment structures can mean that individual institutions are only able to monitor certain aspects of an overall process.

In this context, several interviewees emphasise the importance of institutional cooperation between financial institutions, payment service providers, platform operators and analytical authorities. It is only by bringing together different data perspectives that complex interaction and transaction structures can be assessed comprehensively. International analyses of combating digital financial crime also indicate that effective risk assessments are increasingly dependent on inter-institutional cooperation and data aggregation.

In practical terms, this means the following for the detection of financial transactions in the context of sexualised violence and the exploitation of minors: account-based systems generally provide better points of reference for reporting suspicious activity, thanks to KYC processes and transaction monitoring. In the case of peer-to-peer services and crypto-based structures, however, classifying individual transactions usually requires additional contextual information – such as that derived from platform interactions or network analyses – which is often not immediately available to institutions.

The findings of the study suggest that digital forms of sexualised violence cannot be clearly attributed to any single payment infrastructure. While certain payment methods may be more common in specific contexts, overall, there is a high degree of variation in the payment methods used.

It is evident that perpetrators and criminal groups frequently combine different payment infrastructures and switch flexibly between them. Risk-relevant structures therefore arise less from an isolated examination of individual forms of payment than from the interplay between payment infrastructures, platform interactions and network structures. The analysis of these relationships forms the basis for the typology of recurring patterns of financial interaction developed in the following section.

4.4 Typologies and possible thresholds

The preceding sections have shown that monetary interactions in the digital space are often characterised by recurring combinations of platform interactions, network structures and financial transaction patterns. Based on the analysis of the interviews and the secondary sources consulted, these patterns were consolidated into a series of typologies of financial interaction structures.

The typologies identified do not relate to abstract payment phenomena but rather to structural patterns described by interviewees from law enforcement, the financial sector and social organisations in the context of the sexual exploitation of minors. They reflect the financial logic behind various forms of crime: from the monetisation of depictions of sexualised violence, through sexual exploitation via livestreaming, to FMSE structures.

The typologies do not represent isolated individual cases but rather describe recurring structural patterns which have been described in a similar way by several interviewees and in international analyses. Typologies represent analytical ideal types that have been developed by bringing together perspectives from several sources. Each typology combines three analytical dimensions: the digital interaction context, typical monetisation and payment structures and the institutional observability of transactions. The analysis revealed several overarching typologies.

Platform-based monetisation of digital interactions

→ A first group of typologies concerns monetised interactions within digital platform ecosystems. In these scenarios, communication, interaction and monetisation functions are often integrated directly into platform architectures.

→ Several interviewees described how platforms are increasingly integrating monetisation features such as pay-per-view models, subscription-based access and virtual goods. Monetary transactions can either be processed within the platform itself or arranged via external payment services.

→ A key feature of this typology is the close link between digital interaction and monetary transactions. Monetary activities often appear to be an integral part of regular platform functions and can therefore only be interpreted within the context of the relevant interaction structure.

Fragmented microtransaction patterns

→ Another typology concerns transaction structures characterised by highly fragmented micropayments. Several interviewees pointed out that financial transactions in the digital realm often do not take the form of single, large transactions, but rather of a series of several small amounts.

→ These sequences of transactions may occur at short intervals or extend over longer periods of time. In some cases, recurring payment intervals and package-based payment models were also described.

→ The fragmentation of transactions can mean that individual payments appear unremarkable when viewed in isolation, while structured patterns can only be identified when viewed within the overall context of a series of transactions.

→ In the context of sexualised violence and the exploitation of minors, this pattern may occur in the case of recurring payments for access to exclusive content or gradually escalating demands for payment in the context of FMSE.

Cross-platform interaction and payment structures

→ A third typology concerns scenarios in which digital interactions and monetary transactions are spread across multiple platforms or technical infrastructures.

→ In such cases, an interaction may, for example, begin on one platform, while communication, organisation or payment processing takes place on other platforms or via separate payment services. Several interviewees described how such cross-platform structures can arise, particularly when platforms fulfil different functions, such as communication, community organisation or payment processing.

→ The distribution of interactions and payments across multiple systems can mean that individual institutions are only able to monitor specific aspects of an overall process.

Hybrid payment structures

→ Another typology concerns the combination of different payment infrastructures within an interaction process. Monetary transactions can, for example, initially take place via traditional account-based payment services and then continue using alternative forms of payment.

→ Several interviewees pointed out that such hybrid structures can arise when different payment instruments each fulfil specific functions, such as low-threshold peer-to-peer payments or international transfers.

→ This combination of different payment methods can help to spread transaction structures across several institutional observation levels.

Possible thresholds and indicators

→ The interviews also show that institutional stakeholders use different approaches to identify potentially suspicious transaction patterns. In this context, combinations of several indicators are often examined, such as unusual payment patterns, recurring small amounts or specific platform contexts.

→ However, several interviewees emphasised that individual indicators, when considered in isolation, are of limited informative value. Instead, a combined assessment of several characteristics is often carried out, in which the transaction structure, payment instruments, platform context and other contextual information are considered together.

→ Against this background, rigid thresholds appear to be of limited suitability in many cases. In practice, risk-based assessment approaches are often used, which combine various indicators and contextual information.

At the same time, analysis of the interviews shows that not all digital interaction structures have a pronounced financial dimension. Some interviewees pointed out that certain forms of digital exploitation or violence dynamics may leave only limited financial traces.

In the analysis, such scenarios were deliberately highlighted as the limitations of a finance-centred approach. This applies to non-commercial forms of dissemination of depictions of sexualised violence against minors, where no monetary transactions take place, as well as contact offences (grooming) that are carried out exclusively through communication. A finance-centred analysis therefore primarily examines commercial forms of exploitation and should be understood as one analytical component amongst several, which must be linked to communicative, technical and criminological perspectives. They have been included in the study to provide a comprehensive picture of digital interaction structures, but do not form the primary focus of the financial risk analysis.

The typologies presented show that monetary interactions in the digital space can be characterised by complex combinations of platform architectures, network structures and payment infrastructures. At the same time, the interviews highlight the fact that institutional stakeholders adopt different perspectives and analytical approaches to these structures. Figure 7 summarises these dimensions in a simplified diagram and illustrates how different platform contexts, forms of monetary interaction and payment infrastructures can be interlinked.

In the following section, these findings are therefore discussed in the context of international research and regulatory developments. The aim is to contextualise the empirical observations and assess their significance for prevention, detection and institutional cooperation in the financial sector.

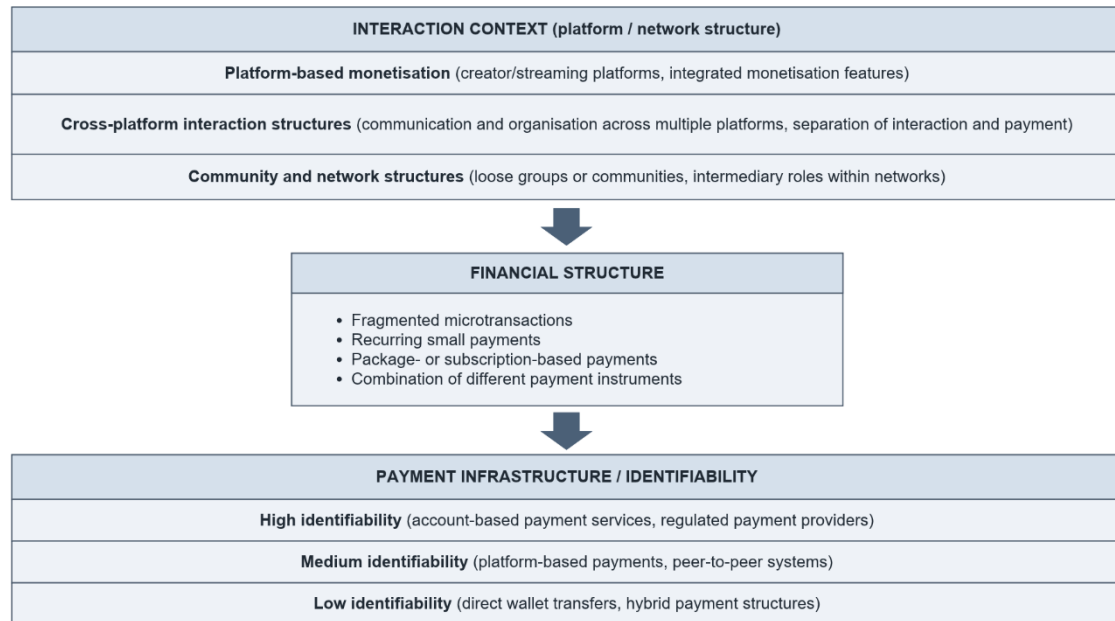


Figure 7: Platform context, monetisation and detectability

V. Discussion and analysis

The empirical findings presented in Section 4 show that monetary interactions in the digital space are characterised by complex combinations of platform dynamics, network structures and financial transaction patterns. The typologies identified make it clear that financial activities cannot be viewed in isolation, but are closely linked to digital spaces for interaction and technical infrastructures.

Against this background, this section aims to place the empirical findings within a broader context and to analyse their significance for existing research approaches, regulatory frameworks and institutional practices. The focus here is on the question of what implications the identified structural patterns have for the analysis, prevention and combating of digital sexual exploitation and the dynamics of violence.

The discussion takes place from several different perspectives. Firstly, the findings are contextualised within existing international research and analytical reports (5.1). The study then examines the significance of the patterns identified for existing AML/CFT frameworks and the practices of financial institutions (5.2). Building on this, the role of digital platforms as structural actors within monetised spaces of interaction is examined (5.3). A further subsection is devoted to the limitations of a finance-centred analysis and the associated methodological and practical challenges (5.4). Finally, the implications for institutional cooperation and governance structures are discussed (5.5).

The aim of this section is not only to describe the empirical findings but also to reflect on their significance in the context of a changing digital ecosystem and to identify starting points for an integrated analysis of the platform economy, financial structures and regulatory mechanisms.

5.1 Context within existing research and international analyses

The empirical findings presented in Section 4 can be linked to a large extent to existing international analyses of digital crime and the financial aspects of exploitative structures. At the same time, however, there are also differences in the analytical focus, particularly regarding the systematic integration of financial perspectives.

The phenomena described by the FATF and Europol refer explicitly to financial structures in the context of the sexual exploitation of minors – in particular commercial forms of online exploitation, monetised livestreaming and FMSE. The present study builds on this offence-specific perspective and expands it to include a systematic analysis of the interplay between payment infrastructures, platform architectures and institutional analytical capabilities.

International organisations such as the Financial Action Task Force (FATF) have repeatedly pointed out in recent years that, in certain contexts, financial transactions can play a significant role in the organisation and maintenance of digital exploitation structures. The patterns identified in this study – in particular, fragmented microtransactions, platform-based monetisation models and hybrid payment structures – confirm this assessment. They highlight the fact that monetary interactions are often an integral part of digital interaction processes and cannot be viewed in isolation.

European analyses, in particular Europol's Internet Organised Crime Threat Assessment (IOCTA), also highlight the growing importance of digital platform economies in the organisation of criminal activities. Platforms therefore function not only as spaces for communication, but also as infrastructure hubs for interaction, organisation and, in some cases, monetisation.

The cross-platform interaction and payment structures described in the interviews, as well as the close link between interaction and monetary mechanisms, are consistent with these observations.

At the same time, this study shows that financial aspects are often analysed less systematically in existing research than communicative and social interaction dimensions. Many studies focus primarily on content, perpetrator profiles or platform dynamics, while the underlying transaction structures and payment mechanisms are often considered only as a secondary matter. The findings of this study therefore help to broaden this perspective by systematically capturing patterns of financial interaction and transactions as a distinct analytical dimension.

Another key finding concerns the importance of payment infrastructures for institutional analytical capabilities. The interviews and the studies analysed all show that different forms of payment not only involve technical differences but also allow varying degrees of traceability and institutional monitoring. This observation is also highlighted in international analyses, which point out that the traceability of financial transactions depends to a large extent on regulatory frameworks, technical infrastructure and access to data.

Furthermore, the findings confirm the fragmentation of information perspectives among different groups of stakeholders, a phenomenon frequently described in the literature. While platform operators primarily collect interaction and communication data, financial institutions hold information on transactions and government analysis and investigation agencies can combine some of these perspectives. The integrated approach to interaction, financial and analytical levels developed in this study brings this fragmentation into sharp focus and demonstrates its practical relevance for the assessment of digital risk structures.

In summary, it can be said that the empirical findings confirm key insights from international research, while offering a more nuanced perspective on the financial dimension of digital interaction structures. In particular, the systematic linking of platform dynamics, monetary structures and institutional perspectives constitutes a complementary analytical contribution to existing research.

5.2 Implications for AML/CFT frameworks and financial institutions

The structural patterns identified in Section 4 have direct implications for existing anti-money laundering and counter-terrorist financing (AML/CFT) systems and for the practices of financial institutions and payment service providers. In particular, it is becoming clear that traditional approaches to transaction monitoring are increasingly reaching their limits when financial activities are closely linked to digital interaction and platform structures.

A key finding of the analysis is that monetary transactions in the digital sphere often do not occur in isolation but are embedded within complex contexts of interaction. However, traditional AML/CFT systems are primarily geared towards the analysis of transaction data and generally have only limited information on the underlying communication and interaction

processes. This creates a structural gap between the observability of transactions and an understanding of their context, which is crucial for the identification of sexual exploitation offences.

The interviews show that fragmented micro-transactions and sequential payment structures can pose a challenge for rule-based monitoring systems. Individual transactions often appear unremarkable, while relevant patterns can only be identified by aggregating several payments or by taking chronological dynamics into account. This increasingly calls for analytical approaches that go beyond the examination of individual transactions and consider sequences of transactions and patterns over longer periods of time.

Furthermore, the findings suggest that platform-based monetisation models and cross-platform interaction structures are blurring the traditional distinction between communication and financial systems. While platforms hold key information about interactions and user relationships, this data often remains beyond the direct reach of financial institutions. Conversely, financial institutions have access to detailed transaction data but only limited contextual information about the underlying interactions. This fragmentation makes it considerably more difficult to carry out a risk-based assessment of individual transactions.

Another key aspect concerns the growing importance of different payment infrastructures and hybrid payment models. The combination of account-based payment systems, peer-to-peer services and crypto-based transactions means that financial interactions are spread across multiple technical and regulatory systems. For financial institutions, this means that individual transactions often represent only part of a wider payment process, which may span various infrastructures.

In this light, both the interviews and international analyses emphasise the need for further development of existing AML/CFT approaches. In particular, effective risk assessments must increasingly be based on integrated analytical approaches that combine transaction data with further contextual information and that must be reviewed and updated on a regular basis. This includes, for example, information about platform interactions, network structures and recurring behavioural patterns. Finally, it was emphasised that the quality of the identification and assessment of suspicious activities depends to a large extent on the available typologies, red-flag indicators and operational guidelines. Supervisory authorities could play a more active role in this regard by providing financial institutions with regularly updated typologies, risk factors and practical guidance on how to proceed. This would not only improve the quality of suspicious activity reports but also enhance legal certainty for the obliged entities and support a more consistent application of risk-based approaches.

At the same time, the interviews suggest that existing AML/CFT frameworks not only have structural limitations but also offer untapped potential for a more nuanced risk analysis. Continuous customer risk classification should be highlighted as a starting point for partially counteracting the contextual shortcomings described. If customer risk profiles are not merely static but are continuously updated and supplemented with risk-based indicators from relevant areas of criminal activity, such as digital sexualised violence, this can help to contextualise transaction patterns more effectively. In such cases, the assessment is not based solely on

individual transactions but takes into account a broader risk profile that also includes behavioural patterns and structural anomalies.

A promising starting point in this regard is the integration of offence-specific risk indicators into existing customer risk classifications. In the context of sexualised violence and the exploitation of minors, this means in practical terms that transaction patterns – such as recurring micropayments to certain platform categories, hybrid payment structures linked to specific user behaviour and sequential payment patterns exhibiting conspicuous temporal patterns – can be incorporated as potential indicators in risk-based analysis procedures. Sexual violence and the exploitation of minors must be recognised as a distinct category of offence in risk assessments and not merely treated as a sub-category of general financial crime.

The interviews suggest that such an approach may, in principle, be helping to reduce parts of the existing "blind spot" in transaction analysis. Particularly when combined with sequence-based analysis and the consideration of platform-specific contextual information, this may yield additional detection opportunities that can lead to suspicious activity reports relating to this type of offence. It must be emphasised, however, that the practical effectiveness of such approaches has so far been the subject of only limited empirical research, and that broader validation – for example, through pilot projects or field studies – would appear necessary.

Against this background, it can be concluded that the further development of AML/CFT systems does not solely involve integration of external data sources but also consistent refinement of existing risk-based approaches within the financial institutions themselves. This highlights the role of financial institutions not only as data providers within the framework of regulatory processes but also as active participants in the further development of analytical methods for identifying complex risk structures.

5.3 The role of platforms and digital ecosystems

The empirical findings presented in Section 4 illustrate that digital platforms play a key structural role within monetised spaces for interaction. Platforms serve not only as the technical infrastructure for communication and interaction but also, increasingly, as the organising – and, in some cases, monetising – entities of digital ecosystems.

Several interviewees emphasised that platforms today fulfil a dual function: on the one hand, they enable interactions between users to be initiated and maintained; on the other, they provide the framework for monetary activities either directly or indirectly. These range from integrated monetisation features to indirect support for transactions via external payment services.

In the context of the sexual exploitation of minors, this dual function is of particular significance: platforms can both create opportunities for offences – for example, by integrating monetisation features that facilitate commercial exploitation – and contribute structurally to concealing such acts if interaction and payment data are not linked or are not passed on to the relevant authorities. The design of platform architectures is therefore not a technically neutral decision but one with specific implications for the protection of children and young people.

A key finding of the analysis is that monetary interactions are often closely linked to platform architectures, even if the actual payment processing does not take place within the platform. In such scenarios, platforms serve as spaces for interaction and coordination, while financial transactions are processed via separate infrastructures. This functional separation of interaction and payment was highlighted in several interviews as a structural feature of digital ecosystems.

At the same time, the findings show that platforms possess information that may be of considerable significance for classifying financial transactions and, consequently, for identifying the types of offence covered by this study. This includes data relating to communication flows, user relationships, interaction patterns and community structures. However, this information is not usually directly accessible to financial institutions, which further exacerbates the fragmentation of observation perspectives previously described in Section 4.3.

International analyses confirm this trend and highlight the fact that platforms are increasingly acting as key players within digital economies. Not only do they shape the technical framework for interactions, but they also influence the opportunities for monetisation and the visibility and controllability of activities within their systems.

Against this background, it becomes clear that analysing monetary interactions in the digital sphere is only possible to a limited extent without taking platform structures into account. While financial institutions primarily analyse transaction data, platform operators have access to complementary information about the context of interactions. The empirical findings suggest that it is only by bringing these different perspectives together that a more comprehensive understanding of digital interaction and payment structures can be achieved.

At the same time, the interviews show that the platforms themselves face considerable challenges. These particularly include the scalability of moderation and control mechanisms, the distinction between legitimate and potentially problematic interactions and the integration of security and preventative measures into existing business models. These areas of tension are also described in international analyses, which highlight the growing regulatory scrutiny of platform ecosystems.

Overall, the findings emphasise the fact that platforms should not be viewed merely as the context for digital interactions but as active structural actors that exert a significant influence over how interactions are organised, monetised and, in some cases, concealed. This has direct implications for the analysis of financial risks and for the design of regulatory and institutional approaches.

5.4 Limitations of finance-centred analysis

The preceding sections have shown that financial transaction structures can provide a relevant analytical perspective on digital spaces for interaction. At the same time, the empirical findings make it clear that a finance-centred approach has inherent limitations and can only partially capture digital interaction and exploitation structures.

A key finding is that not all relevant interactions are necessarily linked to monetary transactions. Several interviewees pointed out that certain forms of digital exploitation or violent dynamics leave only limited immediate financial traces, if any at all. In such scenarios, an analysis based primarily on transaction data reaches its structural limits. This applies to the non-commercial distribution of depictions of sexualised violence against children and young people, where content is exchanged within closed networks without any payment being made, and to contact offences such as grooming, which are primarily organised through communication. By contrast, commercial forms of exploitation – including monetised livestreaming of sexual exploitation, pay-to-view access to CSAM and FMSE – can, in principle, be analysed through financial transaction structures, even though their detection is made considerably more difficult by the fragmentation of data perspectives described above.

Furthermore, the analysis shows that even in cases involving a financial dimension, transactions often represent only part of a broader process of interaction. Monetary activities are typically embedded in communication and network structures that are only partially visible to financial institutions. The fragmentation of data perspectives across platforms, financial institutions and government bodies – as described in the previous sections – means that individual institutions are only able to gather some of the information.

Another aspect concerns the interpretation of transaction patterns. The interviews make it clear that certain structural features, such as microtransactions, recurring payments and cross-platform payment structures, should not be regarded as inherently associated with risk. Similar patterns can also occur in legitimate contexts, including in the field of digital services, platform economies or creator-based business models. This leads to an inherent ambiguity in transaction patterns, which makes a purely finance-based evaluation difficult.

In this light, several interviewees emphasise the importance of contextual information for a nuanced risk assessment. Without additional information about interaction patterns, platform contexts or user relationships, there is a risk that transaction analyses will either remain too vague or lead to an increased number of incorrect assessments. This challenge is also highlighted in international studies, which point to the limitations of isolated transaction analyses.

At the same time, this study shows that the effectiveness of finance-centred analytical approaches depends heavily on the specific payment infrastructure. Differences in the traceability and institutional observability of transactions have a significant impact on the extent to which monetary activities can be tracked and assessed. Infrastructures with limited traceability or fragmented data access make it difficult to link transactions to specific actors, thereby reducing the value of purely transaction-based analyses.

Finally, the interviews suggest that methodological limitations must also be taken into account. This study is based on a qualitative analysis of interviews and secondary sources, the findings of which have necessarily been abstracted and synthesised. The typologies identified therefore represent analytical generalisations and do not constitute a complete picture of all possible forms of interaction and transaction. Further empirical studies, in particular quantitative analyses or institutional pilot projects, could help to further validate and refine the findings presented here.

Overall, it is clear that a finance-centred analysis provides an important, albeit limited, perspective on digital interaction and risk structures. Its strength lies in identifying structured transaction patterns, while its limitations become apparent above all where there is an absence of monetary activity, contextual information is unavailable or transaction patterns remain ambiguous.

5.5 Implications for institutional cooperation and governance

Protecting children and young people from sexualised violence and exploitation in the digital space requires an institutional framework that takes account of the complexity of digital interaction and payment structures. This analysis makes it clear that no single institution can tackle this complexity on its own.

The preceding sections have shown that monetary interactions in the digital space are embedded in complex, cross-platform and institutionally fragmented structures. This leads to a key insight:

no single institution has a complete overview of digital interaction and payment processes.

Rather, relevant information is systematically distributed amongst various stakeholders. This fragmentation particularly concerns the distinction between:

- platform operators who hold interaction and communication data;
- financial institutions that analyse transaction data;
- government analytical and investigative authorities, which are able to collate information from various sources.

The empirical findings suggest that effective approaches to analysis and prevention therefore increasingly depend on the ability to bring these different perspectives together. Institutional cooperation thus becomes not merely a supporting element, but a structural prerequisite for the evaluation of complex digital interaction and financial structures.

International analyses have been highlighting the importance of such cooperation models for several years now. Public-private partnerships are proposed as a key approach to improving the information landscape and developing joint analytical capabilities. This study confirms this assessment and elaborates on it based on the structural patterns identified.

A key area of tension here lies in the differing rationales of the stakeholders involved. Platform operators, financial institutions and government bodies are each subject to their own regulatory requirements, technical frameworks and organisational objectives. These differences can make cooperation more difficult, for example regarding data access, data protection requirements or the interpretation of risk signals.

At the same time, the interviews and the symposium show that existing forms of cooperation – between financial institutions and law enforcement agencies, for example, or in the context of international networks – offer important starting points. In particular, the structured exchange of information, common analytical frameworks and coordinated risk assessment

approaches are cited as key elements. Such approaches demonstrate the potential for cross-sector collaboration between financial institutions, payment service providers, platform operators and public authorities. In the European and German contexts, promoting joint information and analysis platforms and involving international cooperation networks more closely therefore appears to be a promising approach to improving prevention and prosecution.

Another aspect concerns the increasing regulatory oversight of digital platforms. While financial institutions have long been integrated into AML/CFT frameworks, platform operators are increasingly coming under the spotlight of regulatory developments. International initiatives and European regulatory approaches aim to involve platforms more closely in prevention and reporting processes, thereby partially overcoming the separation that has existed to date between interaction systems and financial systems.

Against this background, future governance approaches must increasingly aim to develop integrated ecosystem perspectives. This encompasses not only cooperation between existing stakeholder groups, but also the development of a shared understanding of risk structures, indicators and analytical approaches.

At the same time, the findings make it clear that such integration cannot be achieved through regulatory measures alone. Rather, it also requires further development of technical interfaces, standardised data formats and common analytical models. The challenge lies in combining different data perspectives in such a way that both effectiveness and legal and ethical requirements are taken into account.

In summary, it can be said that the analysis of digital interaction and financial structures is increasingly becoming a collaborative, cross-sector task. The patterns identified in this study highlight the need to overcome existing institutional barriers and to develop integrated governance approaches that take account of the structural characteristics of digital ecosystems.

Ultimately, institutional cooperation in this context is not an end in itself, but a prerequisite for effective protection of minors. The fragmentation of information perspectives across platforms, financial institutions and government bodies reflects a structural protection loophole that cannot be closed by technical and regulatory measures alone. Integrated governance models that systematically incorporate child protection perspectives are therefore not simply one of several possible options but a normative necessity.

VI. Recommendations for action and conclusions

The empirical findings presented in the preceding sections and their interpretation show that monetary interactions in the digital space are characterised by complex, cross-platform and institutionally fragmented structures. Financial transactions are closely linked to digital interaction and communication processes and can only be properly assessed by considering a range of data and analytical perspectives together.

Against this background, the present study identifies several recommendations for action aimed at key stakeholder groups. These relate in particular to financial institutions and payment service providers, digital platform operators and government and regulatory bodies. The aim of this section is to identify specific starting points for further development of existing mechanisms for analysis, prevention and cooperation, based on the empirical findings and the discussion of them.

The following recommendations for action should not be understood as individual operational measures, but rather as structure-based approaches to further development that take account of the specific challenges posed by digital ecosystems. They are based on a synthesised analysis of interviews and international studies and draw on the structural patterns, institutional perspectives and existing limitations of the analysis identified in the preceding sections.

The analysis is structured around key stakeholder groups and cross-sector issues, with a view to identifying both specific and integrated starting points for further development of existing systems.

6.1 Recommendations for the financial sector and payment service providers

The findings of this study show that financial institutions play a key role in analysing monetary interactions in the digital space, while at the same time facing structural shortcomings in information. In this context, there are several areas of focus for further development of existing AML/CFT frameworks.

→ A key lever lies in the further development of risk-based analytical approaches within existing systems. The interviews suggest that continuous and dynamic customer risk classification can help to place transaction patterns more effectively within their contextual framework. By incorporating specific indicators from relevant areas of criminal activity, such as digital sexualised violence against minors, into existing risk models, financial institutions can improve their ability to identify complex patterns that cannot be deduced from individual transactions.

→ Furthermore, the analysis should focus more on transaction sequences and chronological dynamics. Fragmented microtransactions or recurring payment patterns often only reveal their significance when taken in aggregate. Extending existing monitoring approaches to include sequence-based or behaviour-orientated analytical models can therefore make a significant contribution to improving risk assessment.

→ Another area to consider concerns systematic consideration of payment infrastructure and identifiability. The study shows that different forms of payment are associated with varying degrees of institutional traceability. A nuanced assessment of transactions should take these differences into account to a greater extent, for example by applying a risk-adjusted approach to hybrid payment structures or platform-based transactions.

→ At the same time, the results highlight the importance of contextual information beyond pure transaction data. Even though financial institutions do not have direct access to platform data, indirect indicators – such as those derived from customer profiles, behavioural patterns or recurring transaction patterns – can be used to better categorise transactions. This requires greater integration of customer, transaction and behavioural data within existing systems.

→ Furthermore, it is becoming clear that financial institutions must increasingly view their role as part of a wider analytical ecosystem. The effective assessment of complex interaction and transaction structures requires greater cooperation with other stakeholders, in particular payment service providers, analytics companies and government bodies. A structured exchange of information and the development of common analytical approaches can help to reduce existing information gaps.

→ Finally, the interviews show that further development of AML/CFT systems is not merely a technical challenge but also requires organisational and strategic adjustments. These include raising awareness of new risk dynamics, adapting internal processes and continuously developing analytical skills. This is particularly significant in light of the 6th EU Money Laundering Directive, which comes into force in July 2027, in that it broadens the scope of reportable suspicious circumstances compared with the directive currently in force, thereby also paving the way for reporting of suspicious circumstances in the context of the sexual exploitation of minors.

6.2 Recommendations for digital platforms and technology companies

The findings of this study highlight the fact that digital platforms play a key role in the organisation, structuring and, in some cases, monetisation of digital interaction spaces. Against this background, specific requirements arise for platform operators which go beyond traditional content moderation and increasingly take financial interaction structures into account.

→ A key starting point is to give greater consideration to monetary aspects within existing security and moderation mechanisms. The interviews show that interaction and payment processes are often functionally linked, even if the actual payment processing takes place outside the platform. Platforms therefore have access to contextual information that may be highly relevant for assessing financial activities. A more systematic integration of interaction and monetisation perspectives can help to identify potential risk structures at an earlier stage.

→ Furthermore, it becomes clear that platform architectures themselves can influence the organisation of monetary interactions. In this context, platform operators can assess the extent to which design choices and monetisation features create unintended incentives or structural opportunities for problematic contexts of use. Greater integration of child-rights-by-design and safety-by-design approaches into the development of platform features is urgently needed to reduce risks at a structural level.

→ Another important aspect concerns the improvement of internal analytical capabilities regarding network and interaction structures. The study shows that relevant patterns are often not discernible at the level of individual pieces of content or users but only become apparent in the context of interaction networks or recurring behavioural patterns. Platforms can therefore further develop their analytical approaches to identify such structural patterns more systematically.

→ At the same time, the findings highlight the importance of clearly defined interfaces with external stakeholders, in particular financial institutions, research firms and government bodies. As platforms have complementary information, structured forms of information exchange can help to bring together fragmented perspectives. However, this requires an appropriate legal, technical and organisational framework that takes account of both data protection requirements and operational requirements.

→ Another area for action lies in strengthening transparency and reporting systems. Platforms can contribute to the further development of cross-sector analytical approaches by providing structured reports on identified patterns, aggregated observations or general risk dynamics, without disclosing sensitive individual case data.

→ Finally, the interviews show that platforms are increasingly faced with the challenge of distinguishing between legitimate forms of use and potentially problematic interactions. This requires not only technical solutions, but also organisational and procedural adjustments, including through specialist teams, interdisciplinary expertise or the involvement of external partners.

Overall, the findings make it clear that platforms should not be viewed merely as technical infrastructure, but as active shapers of digital spaces for interaction and monetisation. This highlights the need to further develop security, analysis and cooperation approaches accordingly and to align them more closely with the structural characteristics of digital ecosystems.

6.3 Recommendations for action for regulatory and government bodies

The findings of this study highlight that existing regulatory and institutional frameworks are currently unable to keep pace with the structural characteristics of digital interaction and monetisation ecosystems. In particular, the close interconnection between platform interactions, network structures and financial transactions calls for further development of existing governance approaches.

→ A key starting point lies in further developing the regulatory framework to establish a more integrated ecosystem-based approach. While financial institutions are already fully integrated into AML/CFT regimes, digital platforms have so far been subject to different or less specific requirements regarding monetary interaction structures in some cases. The findings of the study suggest that closer integration of financial market regulation and platform regulation is required to address the fragmented data and monitoring perspectives.

→ Furthermore, regulatory approaches should take greater account of the different roles and levels of access to information of the stakeholders involved. Financial institutions, platform operators and government bodies each have their own specific, complementary perspectives on data. Regulatory frameworks can help to link these perspectives together in a more targeted way, for example by promoting standardised exchange formats or clearly defined cooperation mechanisms, including the necessary legal certainty.

→ This recommendation also proposes that regulatory and government bodies should further develop the operational guidelines for the relevant stakeholders. This includes, for example, the provision of up-to-date typologies, red flags and practical guidelines to improve the detection and assessment of suspicious activities, together with clarification of the reporting and audit obligations for financial institutions in relation to transactions linked to the online exploitation of children and swift and comprehensive implementation of the European AML package.

→ Another important aspect concerns the strengthening of public-private partnerships. The interviews and international analyses show that cross-sector cooperation frameworks are a key tool for improving the availability of information and analytical capabilities. Regulatory bodies can provide targeted support for such collaborations through legal clarifications, for example, institutional platforms for exchange or support for joint analytical initiatives. Part of this clarification could, for example, involve confirming that such offences are to be included in the reports of suspected offences submitted in accordance with the new EU Anti-Money Laundering Directive and clarifying relevant issues relating to data protection in the context of inter-institutional and/or cross-border exchanges of information.

→ At the same time, it is becoming clear that the increasing complexity of digital ecosystems is also placing new demands on technical and organisational infrastructures. These include the development of standard data formats, interoperable interfaces and common approaches to analysis and evaluation. Regulatory initiatives can play a coordinating role here by establishing a framework for structured and secure data integration.

→ Another area of focus is support for empirical research and pilot projects. This study shows that many of the structural patterns identified have so far been the subject of only limited quantitative analysis. Regulatory and government bodies can test new analytical approaches and systematically evaluate their effectiveness through targeted support programmes and regulatory sandboxes¹⁰⁰ or cross-sector pilot projects.

→ Finally, the results highlight the need to continually adapt regulatory approaches to the dynamics of digital ecosystems. Digital platforms, payment infrastructures and forms of interaction are evolving at a rapid pace, meaning that risk structures are also subject to constant change. Adaptive and learning-orientated regulation, based on continuous monitoring and adjustment, therefore appears to be a key component of future governance models. Furthermore, the findings suggest that certain minimum standards for digital platforms should be more firmly enshrined in regulation. These include the consistent application of the child-rights-by-design and safety-by-design principles and mandatory completion of risk and impact assessments when introducing new functions or making significant changes to existing platform features. This applies to new monetisation and payment functions, even if these are provided by external payment service providers. An early assessment of potential risks can help to identify unintended opportunities for misuse and to implement appropriate safeguards even at the system design stage.

Overall, the findings highlight that regulatory and government bodies play a key role in shaping integrated approaches to analysis and prevention. The challenge lies in further developing existing frameworks in such a way that they take account of the structural characteristics of digital interaction and financial ecosystems, while at the same time reconciling legal, technical and social requirements.

¹⁰⁰ A regulatory sandbox is a controlled testing environment in which companies, public authorities and regulatory bodies can trial new products, technologies or business models under relaxed regulatory conditions.

6.4 Cross-sector cooperation and data integration

The recommendations for action set out above for individual stakeholder groups make it clear that the analysis and prevention of complex digital interaction and financial structures cannot be carried out in isolation within individual institutions. Rather, the empirical findings point to the need for systematic, cross-sector cooperation that brings together different data perspectives and analytical approaches.

→ A key finding of the study is that relevant information is structurally distributed across different groups of stakeholders. Platform operators have access to contextual information about interactions and networks, financial institutions analyse transaction data and government bodies can bring these perspectives together. This distribution leads to an inherent fragmentation of observability, which can only be overcome through coordinated approaches.

→ In this context, data integration takes on particular significance. The aim here is not to bring together all available information in its entirety but to develop suitable mechanisms for utilising complementary data perspectives in a structured way. This can be facilitated, for example, by standard exchange formats, common analytical models and interoperable technical interfaces.

→ The interviews show that existing forms of cooperation already provide an important foundation but are often still fragmented or project based. One way of taking such approaches further could be to institutionalise cooperation more firmly and to establish long-term structures for sharing information. In this context, both national and international dimensions must be considered, as digital interaction and payment structures are often organised on a cross-border basis. The US-based "Lantern Project" run by the Tech Coalition can serve as a point of reference here. While such international initiatives provide valuable impetus and strategic approaches, successful implementation nevertheless requires systematic adaptation to the specific framework conditions and context of the European Union.

→ Another key aspect concerns the balance between effectiveness and legal and ethical requirements. The exchange and integration of data must be consistent with existing requirements relating to data protection and fundamental rights. Developing suitable governance models that enable both the protection of sensitive data and the effective analysis of complex risk structures therefore presents a significant challenge.

→ The findings of the symposium also make it clear that the effectiveness of existing and future measures does not depend solely on regulatory requirements or technical detection capabilities. Rather, there are significant challenges in operational cooperation between financial institutions, supervisory authorities, financial intelligence units (FIUs) and law enforcement agencies. Legal uncertainties relating to the identification and reporting of suspicious transactions in connection with online exploitation of children were highlighted. As the funds involved often do not originate from traditional prior money laundering offences, there is uncertainty regarding the scope of existing reporting obligations and the permissibility of proactive detection measures. The participants in the symposium therefore identified a significant need for regulatory clarification and for consistent implementation of the European AML package, in particular the extended reporting obligations under the AML Regulation

→ Furthermore, the results show that cross-sector cooperation is not limited to sharing data but also encompasses the development of a shared understanding of risk structures and analytical approaches. Different groups of stakeholders have different perspectives and assessment criteria, which need to be reconciled within the framework of collaborative processes. Joint training programmes, harmonised indicators and interdisciplinary analytical approaches can make an important contribution in this regard.

→ Finally, it is evident that further development of cross-sector cooperation is closely linked to technological developments. Advances in the fields of data analysis, pattern recognition and system integration are opening up new possibilities for identifying complex interrelationships and linking different data sources together. At the same time, these developments require an appropriate regulatory framework to ensure they are used responsibly and effectively.

Overall, the findings emphasise that the analysis of monetised digital interaction structures is a joint endeavour involving various groups of stakeholders. The challenge lies in transforming fragmented perspectives on information into integrated analytical approaches, while not neglecting the respective institutional, legal and technical frameworks. Such an integrated approach forms the basis for the further development of effective prevention and analysis mechanisms in the digital sphere.

Appendix

I. Overview of the expert interviews and written surveys

	Sector	Number	Period
No. 1	Law enforcement	4	Late October – late February
No. 2	Financial sector	8	Mid-November – early March
No. 3	Social organisations	2	Early December – late January
No. 4	Academia	2	Late November – late January

II. Methodology and data documentation

Stage 1: Interview matrix (source level)

To enable a systematic analysis of the interviews, an interview matrix was first drawn up, in which each row represents a source (expert interview or written response). The matrix serves to make the extremely diverse perspectives of FIUs, the police/criminal investigation departments, forensic services, hotlines/NGOs, tech coalitions, payment service providers, banks and crypto service providers comparable within a uniform framework.

The columns of the interview matrix are organised into thematic sections:

→ **Basic metadata.** Recording of the interview ID, name of the institution, type of source (e.g. FIU, police, PSP, VASP, NGO), regional focus and primary role within the ecosystem (e.g. investigative authority, payment service provider, blockchain analytics, hotline). The aim is to ensure that each perspective and area of responsibility is clearly defined.

→ **4Cs framework and focus on offences.** For each source, a code is assigned to indicate whether it primarily reports on Content, Contact, Conduct and/or Commerce. In addition, the nature of the offence is recorded (e.g. distribution of child sexual abuse material, LDCA/OSEC, financially motivated sexual extortion, overlap with human trafficking). This indicates which aspect of the 4Cs framework the institution in question prioritises.

→ **Financial dimension.** This section examines the role played by financial aspects from the perspective of the source (ranging from "a key component of evidence" to "somewhat peripheral"), which payment instruments are relevant (fiat, cards, PSPs, crypto, alternative instruments), which forms of monetisation are described (pay-per-view, subscriptions, microtransactions, token systems, etc.) and which typical patterns regarding amounts and frequency are observed. In addition, broad country- or corridor-based patterns are documented (e.g. buyers from industrialised countries, suppliers in certain high-risk regions).

→ **Platform and ecosystem relevance.** Another section sets out the types of platforms (e.g. livestreaming/creator platforms, social media/messaging apps, gaming, the dark web/leak sites, blockchain ecosystems that the source typically encounters and the role that platform data (hashes, URLs, reports, AI scores) plays in their own work.

→ **Risks, typologies and red flags (from an interview perspective).** This section summarises the main types of risk described by the source (e.g. LDCA, commercial CSAM sites, self-generated CSAM, sextortion, crypto-related payments). In addition, a brief list of typologies (2–5 keywords per interview) is drawn up and a distinction is made between "major" and "sensitive" red flags – that is, indicators that can be operationalised reliably from the source's perspective, as opposed to those that are legally or ethically sensitive.

→ **Detection approaches, cooperation and data situation.** This section outlines the approaches currently used to detect suspicious activity (e.g. rule-based systems, scoring models, blockchain analytics, manual forensics), the implementation status (conceptual, pilot, operational), assessments of false positives/false negatives, the key cooperation partners (FIUs, police authorities, tech coalitions, payment providers and identified gaps in data and cooperation. Finally, the relevance of each interview to the study is described and potential quotations are noted

This interview matrix therefore serves two purposes:

→ It is a documentation tool that ensures the traceability of the analysis.

→ It serves as a springboard for analysis, from which consolidated, cross-source typologies and red-flag clusters are derived as a next step.

Stage 2: Typology matrix (synthesis level)

The second step is to transfer the information from the individual interviews from the source level (Stage 1) to a typological level (Stage 2). While Stage 1 addresses the question "who is saying what?", Stage 2 answers the question "what recurring patterns can be identified across different sources?".

Each row of the typology matrix corresponds to a consolidated typology (e.g. "LDCA livestream via PSP", "Commercial CSAM websites with payment gateways", "Self-generated CSAM & sextortion", "CSAM on blockchain", "P2P crypto with CSAM exposure", "Non-commercial CSAM file-sharing networks" or "Platform-based monetisation in creator/ICAP models").

The columns of the typology matrix include, amongst other things:

Identification and brief description

Typology ID and short title

Concise description in 2–3 sentences (What is happening? Who are the actors? Which platforms?)

Classification within the 4Cs framework and type of offence (e.g. LDCA vs. commercial distribution of CSAM vs. sextortion)

Financial and structural characteristics	Typical payment methods (fiat/PSP, cards, crypto, in-app currencies, tokens)
	Monetisation model (pay-per-view, subscriptions, bundles, micro-transactions, P2P transfers)
	Characteristic transaction patterns (e.g. micro-payments in the double-digit range, package prices, micro-transactions in the blockchain)
	Frequency/timing (one-off payments, batch payments, subscriptions, highly fragmented micro-transactions)
Geography and platform context	Recurring country and corridor patterns (e.g. buyers in industrialised countries, sellers in certain high-risk regions)
	Typical platform context (cam site + separate streaming, dark web marketplaces, social media platforms, creator platforms, blockchain ecosystems)
Risk characteristics and red-flag clusters	Key financial indicators (e.g. recurring small payments to PSPs in specific countries, exposure to known CSAM wallets, suspicious merchant IDs or token purchases)
	Supplementary non-financial indicators (e.g. platform reports, account age, device or IP patterns, information from hotlines or police reports)
	Consolidated red-flag clusters that highlight which combinations of characteristics are particularly significant
Source base and evaluation dimensions	Reference to the interviews on which the typology is based (list of interview IDs from stage 1)
	Assessment of the risk level (e.g. "high" in terms of severity/impact)
	Assessment of the risk of false positives (to what extent do the patterns resemble those of legitimate payments?)
	Assessment of the feasibility of operationalisation for different groups of stakeholders (traditional banks, payment service providers/PSPs, crypto-service providers/VASPs)

This results in a structured set of consolidated risk typologies drawn from many individual contributions, which can be utilised both within the study (text and figures) and as a practical working framework for financial stakeholders and regulators.

Methodology of transfer from Stage 1 to Stage 2

The typologies are derived using a clear, multi-stage process:

→ **Extraction of patterns at the interview level.** First, the key information relating to financial flows, platforms, types of offence and red flags is extracted from each interview. At Stage 1, this information is recorded in the fields "Typologies_Shortlist", "Forms of Monetisation", "Transaction Patterns", "Countries/Corridors", "Red_Flags_HighConfidence" and "Detection_Approach".

→ **Clustering of similar descriptions.** The second step is to consolidate descriptions with similar content across different sources. For example, all information relating to "livestream abuse involving fiat payments from Europe to South-East Asia" (FIU, BKA, PayPal, N26) is incorporated into a joint LDCA livestream typology, even if the interviews vary in their level of detail. The same applies to commercial CSAM websites, sextortion patterns, crypto exposure, etc.

→ **Definition of typological prototypes.** Prototypes are derived from these clusters: each typology is given a clear name, a brief description, a 4Cs classification, the focus of the offence and typical financial and structural characteristics. Contradictions between sources are not smoothed over but documented (e.g. differing assessments of the relevance of cryptocurrency versus fiat); where in doubt, the wording is conservative.

→ **Supplementation with source references and operationalisation questions.** For each typology, the following is recorded:

- which interviews support them;
- how significant the risk impact is in terms of content;
- how high the risk of false positives is considered to be;
- the extent to which different stakeholders (banks, PSPs, VASPs) can apply this typology in practice in the context of monitoring, modelling or manual post-processing. These assessments are based on the statements made by the interviewees and on a comparison of their respective positions within the ecosystem.

→ **Scope and limits of the financial perspective.** Finally, typologies that leave only a very faint financial trail, if any at all (e.g. non-commercial CSAM file-sharing networks) are deliberately flagged as such. They are included in the study to highlight the limitations of a purely finance-centred approach, but are not treated as the primary source of red-flag sets in the financial sector.

Through this two-stage approach – first, systematic structuring of the sources' perspectives in Stage 1, followed by cross-source typological synthesis in Stage 2 – the study remains both methodologically transparent (mapping of the typologies to specific interviews) and practically applicable (clearly formulated patterns that can be operationalised by various stakeholder groups in the financial and platform sectors).

Bibliography

ACAMS (undated). Preventing Online Child Exploitation with Financial Intelligence: An Overview.

Bank for International Settlements (BIS) (2018). Sound practices: Implications of fintech developments for banks and banking supervisors.

Bank for International Settlements (BIS) (2019). Big tech in finance: Opportunities and risks (Annual Economic Report 2019, Chapter 3).

Bank for International Settlements (BIS) (2022). Interlinking payment systems and the role of central bank digital currency (CPMI Paper No. D205).

Bank for International Settlements (BIS) (2023). Annual Economic Report 2023.

Bank for International Settlements (BIS) (2023). Crypto-assets, tokens and DeFi – Navigating the regulatory landscape (FSI Insights No. 49).

Bank for International Settlements (BIS) (2024). Linking fast payment systems across borders: governance and oversight – Final report to the G20.

Federal Financial Supervisory Authority (BaFin) (2024). Auslegungs- und Anwendungshinweise zum Geldwäschegesetz (GwG).

Federal Criminal Police Office (BKA) (2024). Sexualdelikte zum Nachteil von Kindern und Jugendlichen – Bundeslagebild 2024.

CESifo (2017). Shadow Economies Around the World: New Results for 158 Countries, 1991–2015 (Working Paper No. 6430).

Chainalysis (2024). The 2024 Crypto Crime Report.

Childlight (2024). Tackling the rising incidence of financial sexual extortion: Key takeaways from a cross-sector innovation forum.

Council of Europe (2012/2024). Protection of Children against Sexual Exploitation and Sexual Abuse.

ECPAT International (2019). Guidelines on the Implementation of the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography (OPSC): Explanatory Report.

ECPAT International (2020). Summary paper on online child sexual exploitation.

Egmont Group (2018). Public-Private Partnerships (PPPs) from the perspective of Financial Intelligence Units (FIUs).

Egmont Group (2023). Principles for information exchange between financial intelligence units – With glossary.

European Union (2022). Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act).

European Union (2024a). Regulation (EU) 2024/1620 establishing the Authority for Combating Money Laundering and Terrorist Financing.

European Union (2024b). Directive (EU) 2024/1640 on mechanisms to prevent the use of the financial system for the purposes of money laundering or terrorist financing.

Europol (2020). Exploiting Isolation: Perpetrators and victims of online child sexual abuse during the COVID-19 pandemic.

Europol (2023). Internet Organised Crime Threat Assessment (IOCTA) 2023.

Europol Financial Intelligence Public-Private Partnership (EFIPPP) Threats & s and Typologies Working Group (2024). Combating Trafficking in Human Beings through Financial Intelligence: Handbook – 1st Edition.

Financial Action Task Force (2019). Guidance on a risk-based approach to virtual assets and virtual asset service providers.

Financial Action Task Force (2023). Targeted update on the implementation of the FATF standards on virtual assets and VASPs.

Financial Action Task Force (2025). Detecting, Disrupting and Investigating Online Child Sexual Exploitation – Using Financial Intelligence to Protect Children from Harm.

Financial Action Task Force (2012–2025). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – The FATF Recommendations.

Financial Action Task Force (2025). Online Child Sexual Exploitation.

Fry, D., Krzeczowska, A., Ren, J., Lu, M., Fang, X., & Into the Light Index Study Group (2025). Prevalence estimates and the nature of online child sexual exploitation and abuse: a systematic review and meta-analysis.

IAMAT, IJM & IACAT (2020). Online sexual exploitation of children in the Philippines: Analysis and recommendations.

International Monetary Fund (2000). Shadow Economies Around the World (Working Paper WP/00/26).

International Monetary Fund (2004). Financial Intelligence Units – An Overview.

International Monetary Fund (2018). Shadow Economies Around the World: What Did We Learn Over the Last 20 Years? (Working Paper WP/18/17).

International Monetary Fund (2023). Global Financial Stability Report 2023.

International Monetary Fund (2025). Global Financial Stability Report: Shifting Ground Beneath the Calm.

Interpol & ECPAT (2018). Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material – Summary Report.

International Telecommunication Union (ITU) (2023). Measuring digital development: Facts and figures 2023.

International Telecommunication Union (ITU) (2025). Measuring digital development: Facts and Figures 2025.

Katz, M. L., & Shapiro, C. (1985). Network externalities, competition and compatibility.

Lee, J. (2019). Understanding how digital gifting influences social interaction during live streams.

Livingstone, S., & Stoilova, M. (2021). The 4Cs: Classifying Online Risks to Children.

Marques de Sousa, M. (undated). Regulation of Online Child Sexual Abuse: Legal Analysis of International Law & Comparative Legal Analysis.

McKinsey & Company (2025). The 2025 McKinsey Global Payments Report: Competing systems, contested outcomes.

OECD (2024a). OECD Digital Economy Outlook 2024 (Volume 1): Embracing the Technology Frontier.

OECD (2024b). OECD Digital Economy Outlook 2024 (Volume 2): Strengthening Connectivity, Innovation and Trust.

Organisation for Security and Co-operation in Europe (OSCE) (2019). Following the Money: Compendium of Resources and Step-by-Step Guide to Financial Investigations related to Trafficking in Human Beings.

Republic of Austria (2025). Financial Markets Anti-Money Laundering Act (FM-GwG).

Schittenhelm, C., Kops, M., Moosburner, M., Fischer, S. M., & Wachs, S. (2025). Cybergrooming Victimization Among Young People: A Systematic Review of Prevalence Rates, Risk Factors, and Outcomes.

Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., & Hasebrink, U. (2020). EU Kids Online 2020: Survey results from 19 countries.

The Lancet Digital Health (2025). Beyond the social media ban.

Thorn & National Center for Missing & Exploited Children (NCMEC) (2024). Trends in Financial Sextortion: An investigation of sextortion reports in NCMEC CyberTipline data.

UN Committee on the Rights of the Child (2019). Guidelines regarding the implementation of the Optional Protocol on the sale of children, child prostitution and child pornography (CRC/C/156).

UNESCO (2021). Recommendation on the Ethics of Artificial Intelligence.

UNICEF (2024). When Numbers Demand Action: Confronting the global scale of sexual violence against children.

United Nations (1990). Convention on the Rights of the Child.

United Nations Conference on Trade and Development (UNCTAD) (2024). Annual Report 2023: Trade – Unlocking sustainable strategies for people, the planet and prosperity.

United Nations Conference on Trade and Development (UNCTAD) (2024). Digital Economy Report 2024: Shaping an environmentally sustainable and inclusive digital future.

United Nations Office on Drugs and Crime (UNODC) (2009). Global Report on Trafficking in Persons.

United Nations Office on Drugs and Crime (UNODC) (2013). Comprehensive Study on Cybercrime.

United Nations Office on Drugs and Crime (UNODC) (2022). Digest of cyber-organised crime cases (2nd ed.).

United Nations Office on Drugs and Crime (UNODC) (2024). Global Report on Trafficking in Persons 2024.

United Nations Office on Drugs and Crime (UNODC) (2025). Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia.

UN Trade and Development / Swedish Consumer Agency (2025). Key principles on in-game virtual currency – EU Consumer Protection Cooperation Network.

Wittig, P. (2020). Child sexual abuse and exploitation in the digital age – Rethinking §1887 (doctoral thesis).

World Childhood Foundation (2025). Follow the money: Payments for live streaming of child sexual abuse in the Philippines.

Xu, B., et al. (2022). Understanding virtual gifting in live streaming.

Small Amounts, Grave Consequences

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



ECPAT Deutschland e.V.
Arbeitsgemeinschaft zum
Schutz der Kinder
vor sexueller Ausbeutung

