DATA INSIGHT NO 14

LEGISLATION ADDRESSING TECHNOLOGY-FACILITATED CHILD SEXUAL EXPLOITATION AND ABUSE



DISRUPTING HARM

Funded by | Safe Online

Implemented by | ECPAT

In a nutshell:



Significant gaps remain in national laws addressing technology-facilitated child sexual exploitation and abuse, and legislative frameworks often struggle to keep pace with rapid technological developments and the evolving risks they pose to children.



Legal frameworks must be strengthened and future-proofed to respond to evolving technologies, including child sexual abuse material generated by artificial intelligence.



Many countries do not criminalize online grooming in line with emerging international standards.



Sexual extortion of children and the livestreaming of child sexual abuse are rarely addressed through dedicated offences.



Age-related inconsistencies in laws persist, with some frameworks limiting protection to children below the age of sexual consent or excluding older adolescents, despite evidence that they are also significantly subjected to abuse and exploitation.



Outdated terminology such as "child pornography" remains widely used in legislation, despite being misleading and minimizing the abusive nature of the material by framing it as a form of pornography rather than serious sexual crimes against children.

DEFINING TECHNOLOGY-FACILITATED CHILD SEXUAL EXPLOITATION AND ABUSE

The Disrupting Harm project uses the term "technology-facilitated child sexual exploitation and abuse" to refer to situations involving digital, internet and communication technologies at some point during the sexual exploitation or abuse of a child. This type of violence is sometimes referred to as "online" child sexual exploitation and abuse. However, the term "technology-facilitated" is now preferred to convey that this violence against children does not only occur in online spaces; it can occur fully online, or through a mix of online and in-person interactions between perpetrators and children.

LEGAL FRAMEWORKS ADDRESSING TECH-FACILITATED CHILD SEXUAL EXPLOITATION AND ABUSE

According to international and regional human rights instruments, States have particular obligations and responsibilities to ensure that children fully enjoy their rights and live a life free of violence. One important part of these responsibilities is creating legislation that is not only adequate but also tailored, child focused and responsive to the types of harm children are subjected to.

At the same time, legislation alone is not the solution. Laws cannot, on their own, prevent harm or guarantee protection, but they do create the foundation upon which meaningful action, accountability, prevention efforts – including support for individuals at risk of (re) offending – and support systems can be built, provided they are effectively implemented, adequately resourced, and supported by appropriate enforcement and professional capacity. Strong legal frameworks set the direction, define responsibilities, ensure accountability and provide the basis for the broader work needed to protect children in practice.

In this context, a detailed analysis of national legal frameworks addressing tech-facilitated child sexual exploitation and abuse formed one component of the broader Disrupting Harm research project. Cross-triangulation with findings from other research activities made it possible to move beyond law on paper and instead build a more comprehensive picture of how legal frameworks operate in practice, and how they interact with the systems and professionals responsible for prevention, response and accountability, as reflected in the country reports. This brief focuses specifically on alignment with international standards and key legal aspects.

TABLE 1: ASSESSMENT OF LEGISLATION ON SELECTED TECH-FACILITATED CHILD SEXUAL EXPLOITATION AND ABUSE ISSUES IN COUNTRIES WHERE THE SECOND ROUND OF DISRUPTING HARM STUDIES WAS CONDUCTED.

	SRB	MEX	ARM	COL	MNE	BRA	TUN	JOR	MAR	DOM	MKD	PAK
Definition of child sexual abuse material in line with international standards[i]	P	P	P	P	P	P	P	P	P	P	P	P
Mere possession of child sexual abuse material criminalized (no intent to distribute)	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Online grooming of children for sexual purposes explicitly criminalized[ii]	P	Y	P	N	P	P	N	N	N	N	P	Y
Unwanted exposure of a child to sexual content[iii]	Y	Y	P	N	Y	P	N	Y[iv]	P	Y	P	Y

i For the purpose of this analysis, country legislation on child sexual abuse material is considered to be **fully** in line with international standards when the definition of child sexual abuse material: 1) is directly in line with the guidance provided by Article 2(C) of the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography; 2) covers any type of material (i.e. visual – images, videos, drawings – and audio material); 3) also covers material depicting a person *appearing* to be a minor engaged in sexually explicit conduct (Budapest Convention, Article 9(2)); 4) covers computer/digitally generated child sexual abuse material including realistic images of non-existent children (Budapest Convention, Article 9(2)). When some of these requirements are not met, the country legislation is assessed as being **partially** in line with international standards.

ii Please note that country legislation on this point is assessed as **partial** when, although no legal provision *explicitly* criminalizing online grooming of children for sexual purposes exists, existing provisions do cover to a certain extent the actions constituting the online grooming of children for sexual purposes (e.g. arrangement of a meeting, sexually communicating with a child, etc.).

iii Please note that national legislation on this issue is assessed as **partial** where legal provisions addressing unwanted exposure of a child to sexual content do not protect all children regardless of age or impose additional requirements for the offence to be constituted, such as repeated exposure.

iv The legal framework in *Jordan* is assessed as being fully aligned with international standards because it broadly criminalizes sending or transferring any pornographic material (including depicting adults) through information technologies, thereby covering unwanted exposure of a child to sexual content. However, the law considers the transmission of sexual content to a child an aggravating circumstance only where there is proof of intent to lure or sexually exploit the child. As a result, conduct such as cyberflashing may fall outside its scope despite the inherent harm it can cause.

	SRB	MEX	ARM	COL	MNE	BRA	TUN	JOR	MAR	DOM	MKD	PAK
Livestreaming of child sexual abuse explicitly criminalized[v]	P	P	P	P	P	Y	P	N	P	P	P	N
Sexual extortion of children for sexual purposes explicitly criminalized[vi]	N	N	P[vii]	N	Y[viii]	N	N	P	P	Y	Y[ix]	P[x]

CHILD SEXUAL ABUSE MATERIAL: DEFINITIONS AND RELATED OFFENCES

"Child sexual abuse material" refers to various forms of materials – photos, videos, audio, any other recording or representation – that depict acts of sexual abuse and/or focus on the genitalia of a child for sexual purposes. It is important to note that **child sexual abuse material is the preferred term, replacing older terminology such as "child pornography". Although still used in a legal context, the latter term should be avoided as it is misleading and undermines the gravity of these crimes. Its use suggests that visual depictions of child sexual abuse are just another form of pornography and distracts from the fact that they are representations of a serious crime.**[1] **This framing risks diminishing the seriousness of the abuse, trivializing harm or implicitly legitimizing acts that constitute sexual exploitation and/or abuse of children.**

The first international instrument comprehensively prohibiting and defining such material was the 2000 Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, which defined child sexual abuse material as "any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes".[2] In 2001, the Council of Europe's Convention on Cybercrime extended the definition to also include depictions of a "person appearing to be a minor engaged in sexually explicit conduct"[3] and "realistic images representing a minor engaged in sexually explicit conduct".[4] The latter type of material is also known as computer-generated or digitally generated

v Please note that country legislation on this point is assessed as **partial** when, although no legal provision *explicitly* criminalizing livestreaming of child sexual abuse exists, judicial interpretations have indicated how existing provisions on "pornographic performances" also include "performances" that are livestreamed. Hence, livestreaming of child sexual abuse is criminalized but *implicitly*.

vi Please note that national legislation on this issue is assessed as **fully** aligned with international standards where legal provisions explicitly cover both the act of threatening to disseminate sexual images of a child without the child's consent and the purpose of obtaining sexual favours, money or other benefits.

vii The legal framework in *Armenia* is assessed as being partially aligned with international standards because, while it criminalizes blackmailing a person into engaging in acts of a sexual nature or surrendering property, it fails to capture the specific method involved, i.e. the use of threats to disseminate a child's sexual content.

viii The legal framework in *Montenegro* is assessed as being fully aligned with international standards because it criminalizes threats to disclose sexual content depicting a child, with penalties proportionate to the gravity of the offence, thereby ensuring that sexual extortion of children is fully covered irrespective of what the perpetrator seeks to obtain.

ix The legal framework in *North Macedonia* is assessed as being fully aligned with international standards because it criminalizes threats to disclose sexual content depicting a child, with penalties proportionate to the gravity of the offence, thereby ensuring that sexual extortion of children is fully covered irrespective of what the perpetrator seeks to obtain.

x The legal framework in *Pakistan* is assessed as being partially aligned with international standards because, while it criminalizes transmitting any information that intimidates a child with a sexually explicit image or video for the purpose of blackmail, it fails to capture the specific method involved, i.e. the use of threats to disseminate a child's sexual content.

child sexual abuse material and refers to material that, although it may be depicting non-existing children, is so realistic as to create the illusion that real children are involved in the abuse.[5] Most recently, the United Nations Convention against Cybercrime, adopted in 2024, confirms that child sexual abuse material may include visual, written and audio content, while introducing an important development by explicitly covering material depicting children observing sexual activity, as well as material of a sexual nature depicting children subjected to torture or cruel, inhuman or degrading treatment.[6]

Across all countries where the second round of studies of Disrupting Harm was conducted, national legislation only partially reflects internationally recognized definitions of child sexual abuse material. In many cases, the outdated term "child pornography" remains predominantly used. Important gaps also remain in how child sexual abuse material is defined. For example, some countries, like *Colombia*[7] and *Tunisia*[8], do not include depictions of a child's genitalia for primarily sexual purposes within the scope of abusive material. Countries such as *Serbia*,[9] *Montenegro*,[10] *North Macedonia*[11] and *Pakistan*[12] exclude non-visual forms, like audio-only or written content, from the definition of child sexual abuse material. Only *North Macedonia*[13] and *Tunisia*[14] extend their definition to depictions of persons who appear to be children. Clear definitions matter because they shape what can be recognized, investigated and ultimately prosecuted. In addition, provisions on child sexual abuse material determine the types of conduct that can be addressed under the law and whether harmful behaviour taking place online can be adequately responded to.

At a minimum, laws should criminalize the production, distribution, dissemination, import, export, offer, sale and possession (even with no particular purpose or intent to further distribute/use) of child sexual abuse material,[15,16,17] as well as knowingly obtaining access to such material.[18] Across all the countries, the criminalization of conduct related to child sexual abuse material is quite comprehensive, including the prohibition of mere possession (with no intent to use/share further) in all jurisdictions. However, mere access is expressly prohibited only in *Armenia*[19] and *Serbia*,[20] creating a loophole that allows individuals to deliberately seek out and view such content with impunity in the other countries included in this analysis. **While this legal gap may stem from the mistaken assumption that simply "viewing" child sexual abuse material does not cause harm to children, it may also sustain demand for such material and, in turn, contribute to the continued sexual abuse and exploitation of children for its production**. In addition, where livestreaming of child sexual abuse is prosecuted under provisions on child sexual abuse material, the fact that simple access is not criminalized may allow viewers to escape prosecution.

Research suggests that artificial intelligence tools are increasingly being used to create child sexual abuse material. Across nine of the countries participating in the second round of Disrupting Harm research, 2 per cent of children surveyed on average said that someone had used artificial intelligence to create fake sexual images/videos of them. This figure ranged from 0.4 to 4 per cent depending on the country.[xi] Yet in most countries this conduct is not expressly criminalized. **Existing legal definitions of child sexual abuse material often do not encompass digitally generated content, including material created through artificial intelligence or manipulated to simulate a child engaged in sexual activity**. Although the need to criminalize digitally generated child sexual abuse material predates the emergence of generative artificial intelligence, recent technological developments have significantly expanded both the scale and accessibility of such content. This gap is therefore significant, given that such content may facilitate the blackmail and coercion of children or be disseminated in ways that cause serious harm to them. More explicit legal frameworks are therefore needed to ensure that the criminalization of related conduct does not depend solely on open-ended interpretation of provisions on child sexual abuse material.

Clear definitions matter because they shape what can be recognized, investigated and ultimately prosecuted.

xi The countries included in the analysis were Armenia, Brazil, Colombia, the Dominican Republic, Mexico, Montenegro, North Macedonia, Pakistan and Serbia. Jordan is not included in this analysis due to differences in the final survey questionnaire, while Morocco and Tunisia are not included as data were not available for public release at the time this brief was written.

Legislative developments indicate emerging efforts to explicitly address digitally generated child sexual abuse material in some of the countries where the second round of Disrupting Harm studies was conducted. In January 2026 *North Macedonia* amended its Criminal Code to criminalize the creation of new, or the alteration of existing, visual, audio or written material with sexually explicit content relating to a specific person, by using digital or other tools, and the use or dissemination of such material. Where the offence targets a child, perpetrators face aggravated penalties.[21] Similarly, *Brazil*'s Statute of the Child and Adolescent criminalizes altering or tampering with visual content to simulate a child in sexual material, as well as disseminating, acquiring, possessing or storing such material.[22] While this provision does not explicitly cover content generated by artificial intelligence, a bill seeking to include it was under consideration as of early September 2026.[23]

However, it should be noted that none of these provisions extends to digitally generated child sexual abuse materials that do not depict real children, including those generated through tools powered by artificial intelligence. Given that such content may normalize or fuel demand for child sexual abuse material, explicitly criminalizing its production and dissemination would constitute an important step towards strengthening legal responses to this emerging form of tech-facilitated child sexual exploitation and abuse.

ONLINE GROOMING OF CHILDREN FOR SEXUAL PURPOSES AND UNWANTED EXPOSURE TO SEXUAL CONTENT

The Council of Europe's Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (also known as the Lanzarote Convention)[24] and the European Union Directive 2011/93[25] both contain an obligation to criminalize the online grooming or solicitation of children for sexual purposes. These instruments refer to this offence as the proposal, through information and communication technologies, from an adult to a child who has not reached the age of sexual consent, to meet with the purpose of sexually abusing and/or exploiting the child. The United Nations Convention against Cybercrime introduced a more comprehensive approach. It defines the offence as intentionally communicating, soliciting, grooming or making any arrangement through an information and communications technology system for the purpose of committing a sexual offence against a child, including offences related to child sexual abuse material.[26] **This definition fully recognizes grooming as a crime of intent that can take place entirely online**. By removing age-of-sexual-consent thresholds as a defining element of the offence, it also ensures equal protection for all children, regardless of age. As this broader understanding of grooming is emerging as the new international standard, it provides important guidance for aligning domestic legislation with evolving best practices.

Across the 12 countries there is a general lack of provisions on online grooming of children for sexual purposes that are in line with the United Nations Convention against Cybercrime. *Armenia*,[27] *Serbia*,[28] *Montenegro*[29] and *North Macedonia*,[30] while recognizing that grooming may serve not only to facilitate in-person sexual abuse but also to exploit a child for the production of child sexual abuse material, make the offence contingent on a physical meeting or on preparatory steps towards such a meeting. This excludes grooming that results in exploitation and/or abuse occurring entirely online, for example when a child is coerced into producing sexual content but no physical meeting is planned or takes place.

In addition, *Armenia*,[31] *Montenegro*[32] and *North Macedonia*[33] limit grooming to acts committed against children below the age of sexual consent. A similar issue arises in *Brazil*, where children aged 12 to 17 are excluded from the protective scope of the country's otherwise comprehensive

grooming provisions.[34] This approach is connected to earlier legal frameworks and policy traditions, which link grooming offences to the age of sexual consent, and it may, in practice, contribute to differentiated levels of protection for older adolescents. **Such frameworks increasingly fail to align with the realities of tech-facilitated abuse, as Disrupting Harm data indicate that older adolescents are** subjected to tech-facilitated child sexual exploitation and abuse, including **online grooming, at similar, if not higher, levels than younger children.**[35] **This disconnect between legislation and actual patterns of risk leaves older adolescents inadequately protected despite increased exposure**.

Colombia, the *Dominican Republic*, *Jordan*, *Morocco* and *Tunisia* have no dedicated provisions criminalizing online grooming of children for sexual purposes.

In *Mexico*, the **Federal Penal Code** expressly prohibits the use of telecommunications or any means of data transmission to contact a child and request images, audio or video of sexual activities, or acts of a sexual nature, or to solicit a sexual meeting.[36] In *Pakistan*, the **Prevention of Electronic Crimes Act** criminalizes the intentional establishment of, or steps taken toward establishing, a relationship of trust with a child through electronic communications for the purpose of facilitating, soliciting or committing sexual abuse, or producing, sharing or facilitating the distribution of child sexual abuse material.[37]

In both cases, legal provisions apply to conduct against all children, regardless of age, and encompass situations in which exploitation and/or abuse occur entirely online. *Pakistan* closely aligns with the United Nations Convention against Cybercrime by treating grooming primarily as a crime of intent and targeting its earlier stages, recognizing that harm may already occur during phases of manipulation and trust-building.

Age-related limitations are also evident in provisions addressing unwanted exposure to sexual material. Research conducted in the 12 countries showed that it was the most common form of tech-facilitated child sexual exploitation and abuse.[38] Qualitative data further illustrate how perpetrators can use this as a tactic to normalize sexual behaviour and groom children for subsequent abuse. While this underscores the need for specific provisions protecting all children against unwanted exposure, such as those adopted in the *Dominican Republic*,[39] *Mexico*,[40] *Montenegro*,[41] *Pakistan*[42] and *Serbia*,[43] some countries continue to impose restrictive age thresholds that leave older adolescents outside the scope of legal protection. This is notably the case in *Armenia*,[44] *Brazil*[45] and *North Macedonia*,[46] where such acts are prohibited only when directed at children below the ages of 16, 12, and 14, respectively. In addition, *Morocco* requires repeated conduct to constitute the offence,[47] excluding cases involving only one or a limited number of occurrences.

At the same time, it is important that legal and policy responses distinguish between abusive and exploitative conduct and consensual interactions that may occur within age-appropriate romantic peer relationships, rather than treating all forms of exposure or exchange of sexual content between children as inherently unwanted or harmful. A child-centred approach requires recognizing both the realities of abuse and the evolving nature of young people's digital and romantic relationships.

LIVESTREAMING OF CHILD SEXUAL ABUSE

The livestreaming of child sexual abuse refers to child sexual abuse that is perpetrated and viewed simultaneously in real time via communication tools, video conferencing tools and/or chat applications. In many cases, the offender requesting the sexual abuse in exchange for payment or other material benefits is physically in a different location from the children and the facilitators of the abuse.

While the livestreaming of child sexual abuse is not yet explicitly defined in any international conventions, a number of these documents recognize how behaviours involved in this form of tech-facilitated child sexual exploitation and abuse are illegal. In particular, the Convention on the Rights of the Child[48] and the International Labour Organization Convention No. 182 on the Worst Forms of Child Labour[49] recommend that States prohibit "pornographic performances" involving children. In the same vein, the Lanzarote Convention contains a specific article criminalizing all actions concerning the participation of a child in pornographic performances.[50] This form of tech-facilitated child sexual exploitation and abuse may be read as falling within this description as a "pornographic performance".

Most countries where Disrupting Harm was conducted between 2022 and 2026 do not *explicitly* criminalize the livestreaming of child sexual abuse. A few countries such as *Montenegro,*[51] *North Macedonia,*[52] *Serbia*[53] and *Tunisia*[54] have provisions referring to live pornographic "performances" or "scenes". Similarly, the *Dominican Republic* criminalizes the use of children in acts of exhibitionism or in public or private performances for sexual purposes,[55] as well as attending such performances.[56] While these provisions can be broad enough to cover this form of tech-facilitated child sexual exploitation and abuse, including the actions of those who organize, facilitate or watch such abusive activities, the fact that they do not specifically refer to the livestreaming of child sexual abuse may create interpretative uncertainty, potentially allowing perpetrators to avoid prosecution.

The livestreaming of child sexual abuse material may also fall under various existing provisions outlawing child sexual abuse material. This appears to be the case in *Colombia*, where, despite the absence of dedicated provisions, law enforcement representatives consulted during the Disrupting Harm research confirmed that offences relating to child sexual abuse material and sexual acts with children have been used to prosecute such conduct. In addition, the United Nations Convention against Cybercrime contains an obligation to criminalize the transmission of child sexual abuse material through an information and communications technology system, an approach reflected in the legal frameworks of *Mexico*,[57] *North Macedonia*[58] and *Pakistan*.[59] However, this may not always be sufficient to cover the livestreaming of child sexual abuse, given that often no actual "material" is created, downloaded or stored. This issue arises, for example, in *Mexico*,[60] *Montenegro*[61] and *Serbia*,[62] where provisions on child sexual abuse material expressly require the material to exist in the form of "items" or "data files", potentially excluding instances in which sexual abuse is exclusively livestreamed, without resulting in a data file.

Brazil was the only country identified in this round of Disrupting Harm research with dedicated provisions specifically addressing the livestreaming of child sexual abuse. The Statute of the Child and Adolescent prohibits arranging, facilitating, recruiting, coercing or acting as an intermediary to secure the participation of a child in explicit sexual or pornographic scenes, as well as transmitting or facilitating the real-time display or transmission of such scenes online and digitally.[63] While this provision could be further strengthened by explicitly criminalizing access to livestreamed child sexual abuse, it avoids the interpretative uncertainty associated with frameworks that depend on the existence of "material", and therefore provides an example of good practice in addressing this form of tech-facilitated child sexual exploitation and abuse.

SEXUAL EXTORTION OF CHILDREN

Tech-facilitated sexual extortion of children refers to blackmailing a child using sexual material depicting them to extort sexual favours, money or other benefits, under the threat of further sharing the material (e.g. posting images on social media). Often, the influence and manipulation, typical of grooming, turns into a rapid escalation of threats, intimidation and coercion once the child has been persuaded and/or manipulated to send the first sexual images of themselves. While sexual extortion is not yet explicitly defined in any international legal conventions, both the Council of Europe's Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse[64] and the European Union Directive 2011/93[65] contain an obligation to criminalize the use of coercion or threats to engage in sexual activities with a child.

Most countries where the second round of Disrupting Harm studies was conducted do not *explicitly* criminalize the sexual extortion of children in line with the above definition, instead relying on analogous offences for prosecution. In *Brazil*, judges and prosecutors may use provisions related to the dissemination of child sexual abuse material,[66] or to threats and psychological violence against women,[67] insofar as they apply to the coercive dimensions of the conduct.[68] While across countries broader offences relating to extortion, coercion or blackmail may theoretically be used to prosecute sexual extortion, they are often not designed to address situations in which perpetrators seek to obtain sexual material or sexual acts. In the *Dominican Republic*, for example, the Law on High Technology Crimes and Offences criminalizes blackmail carried out through electronic systems only when aimed at obtaining funds or valuables,[69] and similar limitations arise under general blackmail provisions in *Morocco* and *Tunisia*.[70]

In some countries, potentially applicable provisions are framed in overly broad and generic terms, creating a risk of inconsistent judicial interpretation and outcomes. *Colombia*, for example, criminalizes compelling a person to do something for the purpose of obtaining an unlawful benefit for the perpetrator or a third party.[71] In the same vein, *Jordan*'s Cybercrime Law prohibits the use of information technology to blackmail or threaten a person to compel them to act or provide a benefit.[72] While these provisions do theoretically enable the prosecution of sexual extortion, they fail to fully capture the specific harm and methods involved, namely the use of threats to disseminate a child's sexual content as a means of coercing that child into engaging in sexual acts or providing more sexual content, money or other benefits. *Armenia* presents a related issue: Although the Criminal Code criminalizes blackmailing a person into engaging in acts of a sexual nature or surrendering property,[73] it does not specifically reflect the coercive use of such threats. Without a dedicated framework, sexual extortion risks being absorbed into broader offence categories, hindering clear classification and the collection of accurate data on case prevalence.

In January 2026, *North Macedonia* amended its Criminal Code to criminalize threatening another person with sharing sexually explicit materials portraying them, with harsher penalties when that person is a child,[74] joining *Montenegro* in adopting this approach.[75] By centring the offence on the threat of disclosure of sexual content rather than on any particular purpose pursued by the perpetrator, these two legal frameworks ensure that sexual extortion of children is fully covered, irrespective of what the perpetrator seeks to obtain, while also more accurately reflecting the coercive use of self-generated sexual material depicting the targeted child.

CONCLUSIONS AND RECOMMENDATIONS

The analysis of national legislation on tech-facilitated child sexual exploitation and abuse conducted as part of the second round of Disrupting Harm research highlighted that many countries still have significant gaps in the comprehensive criminalization of its various manifestations. As digital environments continue to evolve, legal frameworks should be designed to be future-proof and capable of adapting to emerging forms of harm. The existence of specific legal provisions addressing each form of tech-facilitated child sexual exploitation and abuse would strengthen the protection afforded to children, facilitate the prosecution of offenders and potentially contribute to deterrence. Stronger legislation can also play an important role in prevention by signalling clearly that these forms of harm are serious, recognized and unacceptable. This also includes the importance of language itself. Moving away from outdated terms such as "child pornography" towards terminology such as "child sexual abuse material" better reflects the reality that these materials document sexual abuse and exploitation and can potentially contribute to reduce victim-blaming attitudes within justice systems and society at large.

Moreover, ensuring that tech-facilitated child sexual exploitation and abuse is adequately criminalized, and that penalties associated with these offences are proportionate to their gravity, may help counter the persistent misconception that sexual offences against children committed through digital technologies are less serious than abuse occurring in person. In several interviews with front-line workers and justice professionals conducted as part of the Disrupting Harm research, participants described a "tendency to perceive tech-facilitated forms of child sexual exploitation and abuse as less serious or harmful than offences involving direct physical contact".[76]

A further cross-cutting issue emerging from the analysis relates to age-based thresholds in legal protection. In some contexts, certain offences remain tied to the age of sexual consent, which can result in uneven levels of protection for adolescents despite evidence showing that they are exposed to online risks at higher rates than younger children in 19 out of 21 countries studied by Disrupting Harm.[77]

Each Disrupting Harm country report therefore includes recommendations outlining legislative reforms needed to strengthen national responses to these forms of abuse. The recommendations below build on these country-specific findings and describe broader legal reforms that may be applicable across different legal contexts:



- **Amend legislation to ensure that tech-facilitated child sexual exploitation and abuse can be prosecuted effectively**. This could also support prevention by strengthening deterrence and signalling that all forms of exploitation and abuse are serious crimes. A package of legislative reforms to align with international standards could include the following:
  - Expand and align the legal definition of child sexual abuse material with international standards and technological developments, including by ensuring that the definition covers any type of materials, including non-visual forms such as audio-only content. Legislation should also explicitly include digitally generated, altered or manipulated content, such as material generated with the use of tools powered by artificial intelligence, depicting real as well as non-existent children.
  - Replace the outdated and harmful terminology "child pornography" with "child sexual abuse material" in relevant legislation and criminal provisions. This terminology more accurately reflects the abusive nature of the material and recognizes that such material may be used as a catalyst for further exploitation and abuse, in alignment with the Terminology Guidelines for the Protection of Children from Sexual Exploitation and Abuse.[78]
  - Comprehensively criminalise all relevant conduct involving child sexual abuse material, including its production, distribution and transmission, and the act of making it available, as well as mere possession and intentional access, even where there is no intent to distribute or further share the material.
  - Ensure that legislation comprehensively criminalizes grooming of children for sexual purposes, including situations where the perpetrator does not intend to meet or have physical contact with the child so as to encompass abuse occurring entirely online (e.g. coercing the child to produce sexual content).
  - Adopt explicit legal provisions criminalizing tech-facilitated sexual extortion of children. While criminal provisions on extortion, blackmail or other similar offences may apply in some cases, a dedicated offence supported by a clear definition can better capture its

specific dynamics, including the coercive use of sexual images or videos to obtain sexual acts, additional sexual material, money or other benefits from a child.

– Explicitly criminalize the livestreaming of child sexual abuse, either through a stand-alone provision or by clarifying that offences relating to child sexual abuse material – or other relevant offences – also apply when abuse is streamed in real time without being recorded or stored.



- **Ensure that all children under 18 receive equal protection from tech-facilitated sexual exploitation and abuse**, regardless of their age or gender, including by ensuring that penalties reflect the nature and severity of the offence and the harm caused, rather than the child's age.



- **Ensure that children are not prosecuted for creating, possessing or voluntarily sharing self-generated sexual content with peers, where informed consent and no evidence of coercion, exploitation or malicious intent exist**. The legal framework should clearly distinguish consensual peer activity from exploitative and abusive conduct.



- **Ensure that criminal legislation is sufficiently technology-neutral and adaptable to emerging forms of tech-facilitated child sexual exploitation and abuse**. Provisions should avoid relying exclusively on specific platforms, technologies or methods of offending so that emerging forms of exploitation and abuse can be effectively addressed as technology evolves.

ABOUT THE *DATA INSIGHTS* SERIES FROM DISRUPTING HARM

Disrupting Harm is a research project conceived and funded by Safe Online since 2019. The project and its research methodology is designed and implemented by ECPAT International, INTERPOL and UNICEF Office of Strategy and Evidence – Innocenti (UNICEF Innocenti). This research generates national evidence on tech-facilitated child sexual exploitation and abuse.

This publication is part of a series of thematic briefs that explores pressing issues emerging from the research, and recommends ways for key entities and individuals to improve prevention and response. Evidence about tech-facilitated child sexual exploitation and abuse was collected in 13 countries between 2020 and 2021: seven in Eastern and Southern Africa (Ethiopia, Kenya, Mozambique, Namibia, South Africa, Uganda and the United Republic of Tanzania), and six in Southeast Asia (Cambodia, Indonesia, Malaysia, Thailand, the Philippines and Viet Nam).

In 2024 and 2025, data was collected in an additional 12 countries: Armenia, Brazil, Colombia, the Dominican Republic, Jordan, Mexico, Montenegro, Morocco, North Macedonia, Pakistan, Serbia and Tunisia.

Since 2019, the Disrupting Harm project, together with national partners and researchers, have conducted surveys and interviews with more than 25,000 children and young people, including those who have been subjected to tech-facilitated sexual exploitation and abuse. In addition, over 25,000 caregivers were surveyed, and 540 professionals with child protection mandates interviewed. More detailed information about the Disrupting Harm research methods can be found here.

This specific brief on legislation addressing and criminalizing tech-facilitated child sexual exploitation and abuse covers only the countries that were part of the second round of studies. The related data insight for the first set of countries can be found here.

Data collected by ECPAT, INTERPOL and UNICEF Innocenti since 2019 are used as the basis for the Disrupting Harm Data Insights series. Authorship is attributed to the organization(s) that produced each brief. While the Disrupting Harm project is a close collaboration between ECPAT, INTERPOL and UNICEF, the findings, interpretations and conclusions expressed in this publication are those of the authors and do not necessarily reflect the views of the three organizations ECPAT, INTERPOL and UNICEF, individually or as a collaborative group.

ENDNOTES

1 See Interagency Working Group on Sexual Exploitation of Children, *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*, 2nd ed., ECPAT International, 2025.

2 United Nations General Assembly, Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, Art 2(c) (2000).

3 Council of Europe, Convention on Cybercrime, Art 9(2) (2001).

4 Council of Europe, Convention on Cybercrime, Art 9(2) (2001).

5 Interagency Working Group on Sexual Exploitation of Children, *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*, 2nd ed., ECPAT International, 2025, p. 66.

6 United Nations General Assembly, Convention against Cybercrime, Art 14-2 (2024).

7 Colombia, Criminal Code, Art 218 (2000).

8 Tunisia, Decree-Law No. 54 of 2022 of 13 September 2022 on Combating Offences Related to Information and Communication Systems, Art 26 (2022).

9 Serbia, Criminal Code, Art 185(6) (2005).

10 Montenegro, Criminal Code, Art 211-2, 211-3, 211-7 (2003).

11 North Macedonia, Criminal Code, Art 122(24) (1996).

12 Pakistan, The Prevention of Electronic Crimes Act, Section 22 (2016).

13 North Macedonia, Criminal Code, Art 122(24) (1996).

14 Tunisia, Decree-Law No. 54 of 2022 of 13 September 2022 on Combating Offences Related to Information and Communication Systems, Art 26 (2022).

15 United Nations General Assembly, Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, Art 3(1)(c) (2000).

16 Council of Europe, Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Art 20(1)(e) (2007).

17 Council of Europe, Convention on Cybercrime, Art 9(1)(e) (2001).

18 Council of Europe, Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Art 20(1)(f) (2007).

19 Armenia, Criminal Code, Art 300 (2022).

20 Serbia, Criminal Code, Art 185(4) (2005).

21 North Macedonia, Law on Amendments and Supplements to the Criminal Code, Art 6 (new article 152-a) (2026).

22 Brazil, Statute of the Child and Adolescent, Art 241-C (1990).

23 Chamber of Deputies, Brazil, 'Commission Approves Increase in the Penalty for the Crime of Digital Pornography', 2025.

24 Council of Europe, Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Art 23 (2007).

25 European Parliament and Council of the European Union, Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, Art 6 (2011).

26 United Nations General Assembly, Convention against Cybercrime, Art 15 (2024).

27 Armenia, Criminal Code, Art 202 (2022).

28 Republic of Serbia, Criminal Code, Art 185b(1) (2005).

29 Montenegro, Criminal Code, Art 211b (2003).

30 North Macedonia, Criminal Code, Art 193-b (1996).

31 Armenia, Criminal Code, Art 202 (2022).

32 Montenegro, Criminal Code, Art 211b (2003).

33 North Macedonia, Criminal Code, Art 193-b (1996).

34 Brazil, Statute of the Child and Adolescent, Art 241-D (1990).

35 UNICEF, 'Technology-facilitated child sexual exploitation and abuse in 21 countries', Disrupting Harm Data Insight no. 11, Safe Online, New York, 2026.

36 Mexico, Federal Penal Code, Art 199 Septies (1931).

37 Pakistan, Act No. XXXVII of 2023 to amend the Prevention of Electronic Crimes Act, 2016, Pakistan Penal Code and the Qanun-e-Shahadat, 1984, Section 4, new article 22A (2023).

38 UNICEF, 'Technology-facilitated child sexual exploitation and abuse in 21 countries', Disrupting Harm Data Insight no. 11, Safe Online, New York, 2026.

39 Dominican Republic, Law No. 74-25 Establishing the Criminal Code of the Dominican Republic, Art 179, 180-6 (2025).

40 Mexico, Federal Penal Code, Art 200 (1931).

41 Montenegro, Criminal Code, Art 211-1, 211-4 (2003).

42 Pakistan, The Prevention of Electronic Crimes Act, Sections 21(1)(b), 21(2) (2016).

43 Serbia, Criminal Code, Art 185(1) (2005).

44 Armenia, Criminal Code, Art 201 (2022).

45 Brazil, Statute of the Child and Adolescent, Art 241-D, -I (1990).

46 North Macedonia, Criminal Code, Art 193(1) (1996).

47 Morocco, Penal Code, Art 503-1-1(2), 503-1-2 (1962).

48 United Nations General Assembly, Convention on the Rights of the Child, Art 34(c) (1989).

49 International Labour Organization, Worst Forms of Child Labour Convention (No. 182), Art 3(b) (1999).

50 Council of Europe, Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Art 21(1) (2007).

51 Montenegro, Criminal Code, Art 211-2, 211-4 (2003).

52 North Macedonia, Criminal Code, Art 193(3), 193(4), 193(5), 193(6) (1996).

53 Serbia, Criminal Code, Art 185(2) (2005).

54 Tunisia, Organic Law No. 2016-61 of 3 August 2016 on Preventing and Combating Human Trafficking, Art 2, 23 (2016).

55 Dominican Republic, Law No. 74-25 Establishing the Criminal Code of the Dominican Republic. Art 180-5 (2025).

56 Dominican Republic, Law No. 74-25 Establishing the Criminal Code of the Dominican Republic. Art 182 (2025).

57 Mexico, Federal Penal Code, Art 202(1) (1931).

58 North Macedonia, Criminal Code, Art 193-a(1), 193-a(2), 193-a(3) (1996).

59 Pakistan, The Prevention of Electronic Crimes Act, Section 22 (2016).

60 Mexico, Federal Penal Code, Art 202(1) (1931).

61 Montenegro, Criminal Code, Art 211-6 (2003).

62 Serbia, Criminal Code, Art 185(4), 185(5) (2005).

63 Brazil, Statute of the Child and Adolescent, Art 240 §1, -II (1990).

64 Council of Europe, Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Art 18-1(b) (2007).

65 European Parliament and Council of the European Union, Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, Art 3-5(iii) (2011).

66 Brazil, Statute of the Child and Adolescent, Art 241-A (1990); Dupret, Cristiane, 'Sextortion in Brazilian Criminal Law', 2021.

67 Brazil, Penal Code, Art 147, 147-B (1940).

68 Ministry of Justice and Public Security, Brazil, 'Operation against Inducement and Sexual Self-Harm on Social Media Is Launched', 2023.

69 Dominican Republic, Law on High Technology Crimes and Offences, Art 16, (2007).

70 Morocco, Penal Code, Art 538 (1962); Republic of Tunisia, Criminal Code, Art 283, 284 (1913).

71 Colombia, Criminal Code, Art 244 (2000).

72 Jordan, Cybercrime Law, Art 18 (2023).

73 Armenia, Criminal Code, Art 199, 258 (2022).

74 North Macedonia, Law on Amendments and Supplements to the Criminal Code, Art 6 (new article 152-a) (2026).

75 Montenegro, Criminal Code, Art 175a (1), (3), (5) (2003).

76 UNICEF and ECPAT, 'Access to justice and legal remedies for children subjected to tech-facilitated sexual exploitation and abuse', Disrupting Harm Data Insight no. 13, Safe Online, New York, 2026.

77 UNICEF, 'Technology-facilitated child sexual exploitation and abuse in 21 countries', Disrupting Harm Data Insight no. 11, Safe Online, New York, 2026.

78 Interagency Working Group on Sexual Exploitation of Children, *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*, 2nd ed., ECPAT International, 2025.

Suggested citation:

ECPAT International, 'Legislation addressing technology-facilitated child sexual exploitation and abuse', Disrupting Harm Data Insight no. 14, Safe Online, New York, 2026.

© ECPAT & Safe Online, 2026. Use of this publication is permitted provided the source is acknowledged and that the publication is not used for commercial purposes.

Funding from Safe Online does not constitute endorsement.

Acknowledgements:

This data insight was drafted by Tiago Afonso and Andrea Varrella, ECPAT International. The data analysis that informed this data insight was prepared by Tiago Afonso, Andrea Varrella and Matteo Russo. We acknowledge the contributions of our implementing partners at UNICEF Office of Strategy and Evidence – Innocenti, INTERPOL and Safe Online, and all national partners who made this initiative possible. Full acknowledgements for the Disrupting Harm project can be found here.