

Protecting Children from AI Generated Deepfakes: A Comparative Legal Analysis of India, United Kingdom and The United States of America

Keyaan Sharma
keyaansharma2011@gmail.com

ABSTRACT

The world is growing rapidly and artificial intelligence (AI) is developing even faster. AI is helpful but if it is in the wrong hands it leads to many problems which affect people globally. If AI is wrongly used it leads to cybercrime such as digital frauds, harassment of people through deepfakes, cyberbullying, identity theft, privacy violation, damage to reputation, blackmail, extortion, exploitation of children and many more¹. It is a universal problem that specifically children of the age group of 10 to 17 years since they are mostly active on the internet and due to their young age and lack of knowledge about deepfakes, they get easily targeted by cybercriminals. My research aims to provide information about laws which are present in the countries to counter the above cases mentioned. I compared the legal systems related to protection of children from cybercrime in countries India, United Kingdom and the United States of America. I found the legal gaps which are present in the current laws of respective countries. I gave a united solution which can globally resolve the problem. It is called the digital identity protection order (DIPO). It is a temporary order issued by the special judiciary which will take down the video from all social media platforms. After proper investigation it may either be removed or restored. DIPO has a much simpler legal process and compiles all laws available for cybercrime in one making it easy for the affected as well the judiciary.

INTRODUCTION

AI has become an important tool which helps in education as well as daily tasks. It helps students by explaining complex mathematical problems, helps create educational videos and help them find the data and other important things which they require from the vast ocean of internet thus saving their time. Beyond education AI also helps older adults and younger children to learn and understand new concepts thus acting as a helping hand to all age groups of people¹. Recent developments in artificial intelligence (AI) have helped in the creation of manipulated and false AI photos and videos which are termed as “DEEPFAKES”. Deepfakes are those videos and photos which are made with the help of AI agents. They are very dangerous because they appear so real that most of the population gets fooled and hence come under the trap of cybercriminal². Misuse of AI can pose severe threat to individuals privacy and security.

Sep 2026
Vol 11. No 3.

These risks range from cyberbullying, identity theft to online harassments³. Teenage children on the internet are the most targeted because cybercriminal know that a teen age child is too young and incapable to understand difference between deepfake and reality hence they try to manipulate child brain with the help of deepfakes and create a sense of trust and then take out important information or photos, which they later use to exploit and harass the child⁴. A Deepfakes of victim can mentally harm them because the photos and video which are uploaded online is completely fake which may lead the victim wide character assassination and harassment of the victim on both social media and real life. Many Cybercriminals who create deep fake use VPN which continuously change their live location thus making it difficult to catch the creator of the deepfake and if the creator publish the deepfake on social media and if that deepfake go viral its multiple copies are being made and stored, thus a viral deepfake is impossible to erase completely⁵. This research examines whether the legal system of India, United Kingdom and the United States of America adequately protect the rights of children. Through a comparative legal analysis this paper highlights the strengths, weaknesses and gaps in the legal system of provided countries.

WHAT ARE AI GENERATED DEEPPAKES?

A deepfake is an AI-generated image, video or audio that is fake which makes a person appear to say or do something which they had never actually said or done. It is created using artificial intelligence (AI) to replace or change a person's face, voice, facial expression or movements. Deepfakes can look very real and make the fake content appear authentic¹. AI is like a student, the more photos and videos it sees the more it understands. When a person asks AI to create a deepfake of any photo or videos, AI first studies the unique features of the individual like the lips, eyes, nose and facial structure. Then it creates an image or video with similar features but this time it would be modified according to the person's prompt. AI continuously makes improvements in the deepfakes by analysing patterns, identifying errors, improving accuracy and refining facial features thus making the deepfake more realistic. The more prompts and photos it receives the better deepfakes are being created by AI². Deepfakes are one side of AI. However AI itself is not harmful. It completely depends on the user. An AI is a tool made by humans with the aim to help everyone. The misuse of AI can lead to problems but its proper use has many benefits. AI helps in healthcare by assisting doctors in creating personalized recovery plans for patients, finding patterns in patients data that may be a sign of an illness by acting as a second check for doctors if they have missed any information and many more. AI also helps in Disaster management by predicting natural disasters, providing early warnings so that people have time to evacuate, assists emergency teams by creating rescue plans for fast evacuation and helping authorities make decisions by combining information from weather forecast satellite image and official reports thus reducing workload and easing decision making for authorities³. Even though AI is beneficial, when used irresponsibly it can lead to the creation of hyper realistic deepfake and when published on online platforms they spread misinformation which harms victims' public image, mental and social well being⁴. When deepfakes are used by hackers they lead to financial frauds which eventually leads to loss in trust on genuine and true digital content by the online users as they assume that the data or information provided in the video is wrong⁵. Deepfakes used against

children can give them traumatic experiences because the peers of the child may lack the ability to differentiate between real and fake content which leads them to consider that deepfake is real which eventually leads to bullying of the victim both online and offline⁶.

WHY DO EXISTING LAWS STRUGGLE TO ADDRESS AI GENERATED DEEPFAKES

AI is moving at the speed of a bullet train whereas law moves at a slower pace. Many existing laws were drafted before the development of modern generative AI therefore, they are unable to provide sufficient protection to victims against generative AI¹⁴. When a country tries to create and amend laws related to AI and cybersecurity, AI technology evolves in months, thus the country's legal structure struggles to catch up with the rapid development of AI. This leads to the creation of legal gaps which are exploited by cybercriminals¹⁵. Laws related to AI and the internet take a long time to come into effect because the law undergoes drafting, expert review, legislative debate, amendments, formal approval, and judiciary require time to understand and implement law. By the time all of this happens, new developments in AI take place, making the implemented laws become less effective. In many jurisdictions, there is no specific law for AI-generated deepfakes, hence legal authorities often have to use multiple legal provisions instead of one specific law. Existing cyber laws deal with identity theft, hacking, defamation, privacy violations, fraud and similar offences, but they struggle to address AI-generated videos and images¹⁶. Due to the absence of a universally accepted and comprehensive legal framework for generative AI, there is uncertainty and inconsistency in legal enforcement. Existing laws often punish the consequences rather than regulating the technology itself. Furthermore, one country may treat deepfakes as a privacy infringement while another may classify them as fraud. Since deepfakes are a global issue, the absence of a binding international legal framework makes cross-border enforcement difficult for the victims¹⁷. By the time legal proceedings will start the deepfake would be copied, downloaded and shared by multiple users hence making it impossible to erase the deepfake completely from the internet. This leads to defamation, character assassination, victims can feel emotional distress for the acts which they haven't really done but will have to face consequences. Therefore a stronger and more coordinated law must be developed. Greater international cooperation can improve the proper working of law without any external interference. With experts predicting that creation and misuse of deepfakes will increase heavily thus affecting more people, therefore development of a specific law aimed to counter and regulate AI deepfakes is essential to ensure safety of individuals and society¹⁸.

METHODOLOGY

This research is based on qualitative legal research. The study does not include any surveys, interviews or lab experiments. The research paper focuses on understanding how different legal systems deepfakes by studying the legal and academic sources of the respective country. Data for this paper was collected from the official government website, acts of parliament, policy documents, official reports, reports from international organisations and other legal sources. This research paper aims to study the legal approach of India, United Kingdom, the United States of America. These countries were selected because each

country has a different judicial approach to addressing AI related challenges. After analysing the strengths and limitations of the above countries, the comparative analysis identified common gaps which were exploited by cybercriminals. These observations helped in developing the proposed Digital Identity Protection order (DIPO) as a legal solution to address the common AI generated issue globally.

To make the comparison clear, the same five criteria are applied to India, the United Kingdom and the United States of America. The five criteria are:-

1. Type and scope of deepfake misuse covered by law.
2. Child-specific protection and age coverage.
3. Responsibilities placed on online platforms or intermediaries.
4. Speed and availability of legal remedies.
5. Cross-border effectiveness and coordination.

These criteria were selected because they help compare not only which laws exist but also who receives protection, who has responsibility to act, how quickly legal protection may be available and what happens when the creator, platform or evidence is outside the country.

RESULTS

India

India currently doesn't have a standalone addressing specifically AI generated deepfakes. If there is any issue related to deepfakes actions are taken under existing laws which are addressing cybercrime privacy, data protection and online content. **India's main cyber law is The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, made under the Information Technology Act, 2000¹⁹**, it strengthens India's regulation of AI-generated and synthetic content. The Rules introduce the concept of "synthetically generated information", impose additional rules and requirements to social media platforms and search engines by giving them guidelines to ensure labelling of AI-generated content in certain situations and strengthen procedures for the removal of unlawful deepfakes and other harmful synthetic content. These Rules represent India's first incentive framework specifically addressing AI-generated content and deepfakes. Yet the amendment act remains fragmented because the rules are under the IT Act and it is not an AI law. They mainly impose restrictions on social media and the internet to regulate certain AI-generated content rather than creating a complete legal framework for AI. They focus largely on online platforms. They do not comprehensively regulate AI developers, model creators, or every stage of the AI lifecycle. **India also introduced The Information Technology (Intermediary guidelines and Digital Media Ethics Code). Rules 2021²⁰** were introduced to make online platforms such as social media companies, search engines and messaging apps more responsible for the content shared on their app. These rules initiate that platforms create a system where

Sep 2026

Vol 11. No 3.

users can report harmful or illegal content, respond to complaints within a reasonable time and cooperate with government authorities when legally required. They also encourage platforms to take reasonable steps to reduce the spread of unlawful content, including deepfakes. Despite these provisions, the IT Rules 2021 have certain limitations in addressing AI generated deepfakes. The effectiveness of these rules largely depends on how quickly online platforms detect and remove harmful content. IT rules mainly regulate the responsibilities of online platforms instead of that developer and the creature of deepfakes.

India also passed an act for the Protection of Children from Sexual Offences Act, 2012²⁸. POCSO is especially relevant because it is a child-specific criminal law and defines a child as a person below 18 years of age. Its definition of child pornography includes certain digital or computer generated images which are indistinguishable from an actual child and images which are created, adapted or modified but appear to depict a child²⁸. Section 13 also covers use of a child through electronic, computer or other technology for pornographic purposes and Section 15 addresses storage and distribution of pornographic material involving children²⁸. Therefore sexually explicit AI generated deepfakes involving children may fall within POCSO depending on the facts of the case. However POCSO mainly deals with sexual offences and pornographic material, therefore a non sexual deepfake involving fraud, ordinary identity misuse or other harm may still depend on the IT framework or other applicable laws.

Applying the five criteria to India:-

1. Scope of misuse:- The IT framework can address different online harms while POCSO provides specific protection where the deepfake involves sexual or pornographic material^{19, 20, 28}.
2. Child-specific protection:- POCSO applies to children below 18 and its definition can include certain computer generated or modified sexual material involving children²⁸.
3. Platform responsibility:- The IT Rules place reporting, due diligence and other responsibilities on online intermediaries²⁰.
4. Speed of remedies:- Different forms of deepfake harm may require different procedures and there is not one single urgent remedy for every type of deepfake^{19, 20, 28}.
5. Cross-border effectiveness:- Cases involving a creator, platform or evidence outside India can still require international cooperation²⁶.

United Kingdom

The United Kingdom doesn't have a single comprehensive AI act regulating artificial intelligence. Instead it follows a sector specific approach, where AI generated deepfakes are tried to be regulated by combining existing independent law and nature of harm caused²¹. With the help of **Online Safety Act 2023** which is one of the most significant laws of the United Kingdom with the aim of improving online safety and reducing harmful content on digital platforms. It applies to online services such as social media platforms search users and user to user service. These acts require these online services to identify and reduce the risk of illegal and harmful content by introducing appropriate safety measures. This act gives Office of Communication (Ofcom), The UK's online safety regulator, the authority to monitor compliance and take

action against companies which fail to meet their requirements. The Online Safety Act mainly applies to those services that fall within the UK's legal jurisdiction. However AI-generated deepfakes can be created and distributed through websites or services operating outside the United Kingdom. Although the Act establishes legal duties for online platforms, the methods used to identify, assess, and remove harmful content are not identical across all services. Different platforms have different moderation technologies and internal policies which may compromise protection of its users. The United Kingdom also introduced Data Protection Act 2018, along with The UK General Data Protection Regulation (UK GDPR) forms United Kingdom's Data protection framework²². It regulates how organisations collect, use, store and share data while protecting individuals privacy rights. This act offers individuals important rights over their personal data including the right to access their data, also have the right to delete their photos or any content related to them from any digital platform if they wished. The Data Protection Act 2018 protects individuals personal data by getting online organisations to handle personal information more responsibly and securely. Hence it strengthens the protection persons photographs, videos and voice recording that could wrongly be used to create AI generated deepfakes. The Data Protection Act mainly protects personal data during its collection and processing but it does not establish clear legal requirements for developers to design AI systems with safeguards against generating deepfakes. As a result the act focuses more on how personal data should be handled rather than establishing a comprehensive reliable legal framework to regulate how AI systems are designed, developed and used to prevent generating synthetic content. Also the act provides protection only when AI generated deepfakes involve identifiable personal data. However some Ai generated content may still cause the spread of misinformation, manipulation without falling within the given legal scope of personal data. Thus in such a situation the act alone cannot provide a complete legal aid.

Applying the five criteria to the United Kingdom:-

1. Scope of misuse:- The Online Safety Act and data protection framework address different forms of online harm and personal data rather than creating one offence for every deepfake^{21, 22}.
2. Child-specific protection:- The online safety framework contains duties aimed at protecting children while data protection law provides another layer of protection for personal information^{21, 22}.
3. Platform responsibility:- Online services have legal responsibilities to identify and reduce risks from illegal and harmful content²¹.
4. Speed of remedies:- The remedy available can depend on the type of harmful content and the process used by the platform or regulator²¹.
5. Cross-border effectiveness:- Content created or hosted outside the United Kingdom can still create practical problems when foreign actors or evidence are involved²⁶.

United States of America

The United States doesn't have a single comprehensive legal framework against AI intelligence and deepfakes. Instead, it relies on a combination of federal laws, state legislation and existing legal principles to address different forms of AI related harm caused. Recent federal legislation has strengthened protection against certain AI generated deepfakes while several states of America have enacted additional laws to regulate specific forms of synthetic media. America has introduced **Take it Down Act 2025** which makes it a punishable offence to knowingly publish content related to a person without the permission of them and it also requires online platforms to remove the reported content within a specific time period²³. It strengthens legal protection for victims of AI generated deepfakes across the United Nation. It is a legal protection across the United States against the non consensual publication of intimate Ai generated deepfakes. This gives victims better protection instead of depending only on different state laws. The act makes it compulsory to remove reported non consensual intimate deepfakes within 48 hours. This helps reduce the spread of harmful content and allows victims to receive quicker protection. Even though it has broad coverage it is still lacking in providing a unified protection because it specifically focuses on non-consensual intimate deepfakes only which is required but other issues like AI deepfakes spreading political misinformation, financial fraud, identity theft. Also the act mainly focuses on removing harmful content after it is shared. It does not create a complete set of legal duties for AI developers to reduce the creation or misuse of harmful synthetic content.

State laws provide another layer of protection in the United States. California Civil Code Section 1708.86 allows legal action concerning certain digitized sexually explicit material and specifically covers situations where the depicted individual did not consent or was a minor when the material was created²⁹. Texas Penal Code Section 21.165 regulates the unlawful production or distribution of certain sexually explicit deep fake media and its current definition includes media created or altered through software, machine learning, artificial intelligence or other computer generated methods³⁰. Virginia Code Section 18.2-374.1 defines child pornography to include certain sexually explicit visual material where an identifiable minor's image was used in creating, adapting or modifying the depiction and for one part of the definition the minor depicted does not have to actually exist³¹. These examples show that state laws can target specific forms of AI generated or manipulated content but the protection still differs from state to state.

The United States of America also has **Children Online privacy protection Act (COPPA)**²⁴ it is a federal law that protects personal information of children under that age of 13. Thus it made websites and online services to obtain parental consent before collecting, using or sharing child personal information. Although COPPA was created before AI became common, it remains one of the most important laws for protecting children's data in the digital environment. COPPA helps protects children's personal information by requiring parental consent before website and online services collect and use the data. This reduces the risk of children's data being misused. The Act encourages online services to handle children's personal information carefully and follow clear privacy rules, helping create a safer online environment for children. All of these factors mainly protect children's personal information. It does not

directly regulate the creation or misuse of AI generated deepfakes involving children. The act applies to children under 13 years of age. Older teenagers who may also become victims of AI generated deepfakes do not receive the same protection under the law.

Applying the five criteria to United States of America:-

1. Scope of misuse:- Federal and state laws regulate specific harms instead of placing every type of deepfake under one comprehensive law^{23, 29, 30, 31}.
2. Child-specific protection:- COPPA protects online personal information of children under 13 while other laws can protect minors from specific forms of harmful synthetic material^{24, 29, 31}.
3. Platform responsibility:- The TAKE IT DOWN Act requires covered platforms to provide a process for removal of qualifying non consensual intimate material²³.
4. Speed of remedies:- The TAKE IT DOWN Act provides a 48 hour removal period for material covered by that law but this does not apply to every kind of deepfake²³.
5. Cross-border effectiveness:- Different federal and state rules already create multiple legal routes and foreign creators, platforms or evidence can make international cases more difficult²⁶.

WHY CAN'T EXISTING LAWS BE USED TOGETHER?

After reading my comparative analysis a common question must have arisen that “why can’t we just simply use all the existing laws together instead of creating a new legal framework”. The simple answer is that many laws already exist which are made for different purposes: some protect privacy, some regulate online platforms, while others deal with cyber crime, data protection etc. As a result victims often have to depend on multiple different laws²⁵. Thus making the legal process more complicated, slower and sometimes confusing. To understand the issue more precisely we shall think of an example where a deepfake of a 14 year old child from India is created by an anonymous person in Indonesia using a platform hosted outside the European Union. The video is then widely shared in Nepal and Bangladesh where EU AI Act doesn’t apply this limits the law which should be universally accepted but isn’t thus that even strong regional law may face practical challenges. Even if the family reports the content to the Indian authorities, they may face difficulties in identifying the creator, taking legal action across different countries and obtaining quick solutions because the creator is outside India's jurisdiction. This example shows that simply combining existing laws cannot solve cross border challenges. It requires much International cooperation and a coordinated legal framework that can work in all countries²⁶.

DIGITAL IDENTITY PROTECTION ORDER ACT (DIPO): A PROPOSED LEGAL FRAMEWORK

The Digital Identity Protection Order Act (DIPO Act) is a proposed international legal framework designed to protect children from AI-generated deepfakes by creating a faster, simpler and more coordinated legal process. Every country that adopts the Act shall establish a National DIPO Centre

(NDIPC) with both offline and online services. The offline centres ensure that children and families who do not have internet access can receive legal help in person, while the online system allows complaints to be submitted immediately from anywhere around the world. Every National DIPO Centre aims to complete the review of urgent complaints involving children within two hours only when sufficient information has been submitted. If the Centre finds that there is an immediate risk of harm to identity. It may issue a Temporary Digital Identity Protection Order (TDIPO) to preserve digital evidence and request the rapid spread and removal of the harmful content while the legal process continues. Once a lawful TDIPO is issued, it shall immediately be sent to the relevant online platform or AI service. Any platform or AI developer operating in a country that has adopted the DIPO Act shall recognise and respond to the lawful order by taking the action required. This creates one common procedure for participating countries and allows online platforms to respond more quickly instead of following different reporting systems in every case. To ensure that every country can implement the Act effectively, an International DIPO Fund shall be established. Every participating country shall contribute annually according to its economic capacity using an agreed formula based on its Gross National Income (GNI)²⁷.

ANNUAL CONTRIBUTION = COUNTRY'S GNI × AGREED DIPO CONTRIBUTION RATE

The contribution rate shall remain the same for all participating countries since it is calculated as a percentage of GNI countries with stronger economies will contribute more, while countries with smaller economies will contribute proportionately less. This creates a fair funding system without placing an unreasonable financial burden on any country. The Fund shall be used to establish and operate National DIPO Centres, train staff, improve technology, support lower-income countries, strengthen international cooperation and ensure that every child has equal access to protection regardless of where they live. The DIPO Act is designed as an international legal framework that countries may adopt through their own legal systems. By adopting the Act, countries agree to follow the same DIPO standards while continuing to apply their own national laws. Any online platform or AI developer providing services in a participating country shall follow the DIPO Act. This allows countries with different legal systems and companies with different policies to work under one common legal framework while respecting their own domestic laws. A child, parent, guardian, school or authorised authority may report a complaint to the National DIPO Centre. Rather than creating new agencies the Centre shall work with existing cybercrime units, digital forensic experts and law enforcement agencies whenever specialised technical assistance is required. This allows countries to use their existing expertise while reducing unnecessary costs and avoiding duplication of resources. The Temporary DIPO also helps to ensure important digital evidence is preserved from the beginning of a case this therefore minimises the risk of evidence being deleted or changed before it can be considered by the court. However the Temporary DIPO does not determine whether a person is guilty or not, that decision is always reserved for the court. An international DIPO Review Committee shall recommend periodic updates for the Act, which participating countries may adopt through their own legal system, with this DIPO intends to bind with the current laws of every country, thus acting as an additional layer of safety through a modified legal framework that supports

current legal system instead of replacing them with this DIPO Act aims to strengthen protection of children from AI generated deepfakes around the world.

LIMITATIONS

Even though DIPO Act tries to address major problems but it also depend on certain factors which are, The Act can only work in those countries who adopt it even with simplified methods some countries may decline to adopt it which can make cross border enforcement slower perhaps more difficult. Establishing National DIPO Centres, training staff and maintaining secure technology may be challenging for lower income countries. Also AI tools continue to evolve quickly DIPO Act may require regular updates to address new forms of AI generated deepfakes and emerging technology. DIPO Act has not yet been implemented or tested therefore its effectiveness can only be evaluated after real world adaptation.

CONCLUSION

While artificial intelligence has provided society with many positive opportunities, it has also facilitated the ability to create harmful deepfakes that may negatively impact children. My research found that India, the United Kingdom and the United States have implemented steps to combat privacy, cybercrime, online safety and data-protection concerns. However since most laws serve different purposes, it can be difficult for individual countries to act quickly and in unison when AI-generated deepfakes spread from nation to nation. Additionally the comparative analysis found that depending on current laws could further complicate legal action, particularly with international cases. As technology continues to advance, international cooperation will play an even more significant role in protecting children in a swift manner no matter where the targeted content originated. To help improve how current laws could work together to protect children from AI-generated deepfakes, I have proposed the Digital Identity Protection Order Act (DIPO Act). The DIPO Act would act as another international framework that complements each country's current laws. Creating a standard reporting process, allowing countries to work with one another and holding the best interest of the child to react quickly can limit the waiting period while still allowing each country to operate within their own laws. While the DIPO Act is only a proposed solution and would need global collaboration to enforce, it is one way to potentially strengthen global legal safeguards for children from AI-generated deepfakes.

REFERENCES

1. UNESCO – Recommendation on the Ethics of Artificial Intelligence

<https://www.unesco.org/en/legal-affairs/recommendation-ethics-artificial-intelligence>

2. UNICEF – Child Safety Online (Official)
<https://www.unicef.org/digitalimpact/what-we-do/child-safety-online>
3. UNESCO – Recommendation on the Ethics of Artificial Intelligence
<https://www.unesco.org/en/legal-affairs/recommendation-ethics-artificial-intelligence>
4. Council of Europe – Artificial Intelligence
<https://www.coe.int/en/web/artificial-intelligence>
5. UNESCO – Recommendation on the Ethics of Artificial Intelligence
<https://www.unesco.org/en/legal-affairs/recommendation-ethics-artificial-intelligence>
6. UNICEF – Keeping Children Safe Online (Official)
<https://www.unicef.org/protection/keeping-children-safe-online>
7. Budapest Convention on Cybercrime
<https://www.coe.int/en/web/cybercrime/the-budapest-convention>
8. Council of Europe – Artificial Intelligence
<https://www.coe.int/en/web/artificial-intelligence>
9. NIST – Artificial Intelligence
<https://www.nist.gov/artificial-intelligence>
10. UNESCO – Recommendation on the Ethics of Artificial Intelligence
<https://www.unesco.org/en/legal-affairs/recommendation-ethics-artificial-intelligence>
11. Council of Europe – Artificial Intelligence
<https://www.coe.int/en/web/artificial-intelligence>
12. Europol – European Cybercrime Centre (EC3)
<https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3>
13. UNICEF. *Keeping Children Safe Online*.
<https://www.unicef.org/protection/keeping-children-safe-online>
14. UNESCO – Recommendation on the Ethics of Artificial Intelligence
<https://www.unesco.org/en/legal-affairs/recommendation-ethics-artificial-intelligence>
15. OECD AI Principles

<https://oecd.ai/en/ai-principles>

16. Council of Europe – Artificial Intelligence

<https://www.coe.int/en/web/artificial-intelligence>

17. Budapest Convention on Cybercrime

<https://www.coe.int/en/web/cybercrime/the-budapest-convention>

18. UNESCO – Recommendation on the Ethics of Artificial Intelligence

<https://www.unesco.org/en/legal-affairs/recommendation-ethics-artificial-intelligence>

19. India Code

<https://www.indiacode.nic.in>

20. Ministry of Electronics and Information Technology (MeitY)

<https://www.meity.gov.in>

21. Online Safety Act 2023 (UK)

<https://www.legislation.gov.uk/ukpga/2023/50/contents>

22. Information Commissioner's Office (ICO)

<https://ico.org.uk>

23. Congress.gov

<https://www.congress.gov>

24. FTC – Children's Online Privacy Protection Rule (COPPA)

<https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa>

25. Budapest Convention on Cybercrime

<https://www.coe.int/en/web/cybercrime/the-budapest-convention>

26. Budapest Convention on Cybercrime

<https://www.coe.int/en/web/cybercrime/the-budapest-convention>

27. World Bank – Gross National Income (GNI)

<https://data.worldbank.org/indicator/NY.GNP.MKTP.CD>

28. India Code – The Protection of Children from Sexual Offences Act, 2012

Sep 2026

Vol 11. No 3.

<https://www.indiacode.nic.in/bitstream/123456789/2079/1/AA2012-32.pdf>

29. California Legislative Information – California Civil Code Section 1708.86

https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV§ionNum=1708.86

.

30. Texas Legislature – Texas Penal Code Section 21.165, Unlawful Production or Distribution of Certain Sexually Explicit Media

<https://statutes.capitol.texas.gov/Docs/PE/htm/PE.21.htm#21.165>

31. Virginia General Assembly – Code of Virginia Section 18.2-374.1, Production, Publication, Sale, Financing, etc., of Child Pornography

<https://law.lis.virginia.gov/vacode/title18.2/chapter8/section18.2-374.1/>