ARTIFICIAL INTELLIGENCE, DIGITAL RIGHTS, AND CHILD PROTECTION

Contemporary Legal Perspectives on Data, Cyberspace, and Screen Regulation

Farabi Yayınevi

ARTIFICIAL INTELLIGENCE, DIGITAL RIGHTS, AND CHILD PROTECTION

Contemporary Legal Perspectives on Data, Cyberspace, and Screen Regulation- 2026

ISBN: 978-625-91851-6-3

DOI: 10.5281/zenodo.22143929

August/ 2026

Ankara, Türkiye

Date: 20.08.2026

Farabi Publishing House
Ankara, Türkiye
www.farabiyayinevi.org

adopted by Esra KOÇAK
ISBN: 978-625-91851-6-3

ARTIFICIAL INTELLIGENCE, DIGITAL RIGHTS, AND CHILD PROTECTION

Contemporary Legal Perspectives on Data, Cyberspace, and Screen Regulation

AUTHORS

Moses Adeolu AGOI

Dr. Olayemi Grace ABIMBOLA

Hoang Le BUU

Nguyen Huynh Ngoc ANH

Vo Thi TAM

Le Nguyen Thao UYEN

Prerna ARORA

Sadhna JAIN

TABLE OF CONTENTS

PREFACE

Artificial intelligence, digital rights, personal data protection, and child safety in cyberspace have become among the most important legal issues of the contemporary digital age. As technological systems increasingly influence communication, governance, education, privacy, identity, and daily life, legal scholarship is required to respond to new forms of risk, responsibility, and protection.

This book, entitled *Artificial Intelligence, Digital Rights, and Child Protection: Contemporary Legal Perspectives on Data, Cyberspace, and Screen Regulation*, brings together academic chapters that examine the relationship between law and digital transformation from different yet interconnected perspectives. The chapters included in this volume focus on artificial intelligence and legal responsibility, the protection of personal image as a form of personal data in cyberspace, and the regulation of children's screen time within developing digital protection frameworks.

The first chapter discusses law in the age of artificial intelligence and addresses key legal questions concerning accountability, transparency, regulation, algorithmic decision-making, and the future of AI governance. The second chapter examines the protection of personal image in cyberspace, emphasizing the relationship between personality rights, personal data, biometric identification, and the right to control one's digital identity. The third chapter focuses on children's screen time regulation and provides a comparative legal perspective with particular reference to India's developing digital protection framework.

Together, these chapters demonstrate that digital transformation cannot be evaluated only as a technological development. It is also a legal, ethical, social, and human rights issue. The protection of individuals in digital environments requires responsive legal frameworks that can balance innovation with dignity, privacy, accountability, and child protection.

It is hoped that this book will serve as a valuable academic resource for researchers, legal scholars, students, policymakers, and all readers interested in artificial intelligence, digital rights, data protection, cyberspace governance, and the legal protection of children in digital environments.

Farabi Publishing House
August 20, 2026
Türkiye

CHAPTER 1
LAW IN THE AGE OF ARTIFICIAL INTELLIGENCE

Moses Adeolu AGOI[1]
Dr. Olayemi Grace ABIMBOLA[2]

[1]Lagos State University of Education, Lagos Nigeria, agoi4moses@gmail.com, ORCID ID: 0000-0002-8910-2876
[2]Lagos State University of Education, Lagos Nigeria, Abimbolaog.@lasued.edu.ng, ORCID ID: 0009-0000-0139-3481

INTRODUCTION

Artificial intelligence, or AI, has become a socio-technological phenomenon that is rapidly changing governance, economics and legal frameworks around the world from a specialised computational discipline (Russell and Norvig, 2021). AI has gone beyond being just a tool for experimental computing and theoretical problem-solving to permeate the fabric of everyday systems and operations, such as in recommendation systems, autonomous vehicles, predictive analytics, and extensive decision support systems. It has become more and more institutionalized and is no longer only a technical innovation but is part of the structure of modern governance and economy and affects state regulation of behaviour, resource allocation and the administration of justice.

The use of AI in areas like health, finance, criminal justice and public administration has been heavily criticized for its lack of accountability, transparency and regulatory preparedness (Calo, 2015; Wachter et al., 2017). In health care, for example, algorithmic systems of diagnosis can have life-changing implications for clinical decision making, and the logic of their decisions can be ambiguous. In financial systems, AI-powered credit-scoring and trading algorithms can decide who gets a loan or cause markets to fluctuate within microseconds. In financial systems, AI can make decisions about access to capital or market volatility within milliseconds, in the case of credit-scoring and trading algorithms. Likewise, in the criminal justice and public administration sectors, predictive policing tools and risk assessment algorithms influence policing strategies and sentencing recommendations, often without users being able to see the logic in and data assumptions behind the tools.

Traditionally, the law has been based on the assumption of human agency which means that liability and responsibility are placed at the level of individuals or institutions that are identifiable (Hart, 1968). The notion of a legal doctrine like "negligence," "intent" and "causation" assumes that human actors have a measure of control over choices and can be held responsible for harm that follows from their choices. AI systems, however, bring in algorithmic autonomy, which makes it difficult to make causal attributions, and thus makes traditional principles of negligence, foreseeability and intent more problematic (Crawford, 2021).

The accountability of AI systems can be split between different parties, such as those who develop the system, provide the data on which it operates, deploy it, and use it. This has been perceived as the "responsibility gap" in which harmful effects arising from AI systems are difficult to trace to any specific human actor (Danaher, 2016). The responsibility gap also poses important normative issues, such as what happens when no one has full responsibility over the behaviour of the system and who should be held legally accountable if there is harm? Distributed causation is not easily fit into traditional liability frameworks, particularly when decisions are made using a probabilistic mechanism, such as a deep learning system. Furthermore, AI systems often behave as "black boxes", even their creators are not able to explain the reasons behind the decisions that are made in the system (Goodfellow et al., 2016). This opacity can be a significant issue in high-stakes settings where rights and obligations are impacted, such as in the legal field. Although decisions about people's rights and opportunities are often made through the use of judicial sentencing tools, employment screening systems and credit scoring algorithms, the rationale for these decisions may not be available. This poses significant due process issues, including that of receiving a reasoned explanation and challenging unfavourable decisions (Pasquale, 2015; Selbst & Barocas, 2018). Algorithmic decision making may have a negative impact on procedural fairness, which is a core tenet of contemporary legal systems, because people are left with little ability to question and challenge the decision they have been made. (Waldron, 2016). Meanwhile AI systems can also perpetuate structural inequities as they are designed using historic data that frequently reflects the structural inequities of society that have been present for a long time (O'Niel, 2016). AI can, in fact, amplify and reproduce discrimination at scale without removing any human bias, and can be structurally embedded into automated systems that seem objective but are actually biased. Some empirical research has shown the discriminatory effects of predictive policing tools, facial recognition systems and algorithmic hiring platforms, such as marginalised racial and gender groups (Buolamwini & Gebru, 2018; Angwin et al., 2016). The results show that algorithmic neutrality is more of an illusion and algorithmic systems must be thoroughly audited and regulated to prevent issues of unfairness and violation of equality principles.

To address these issues, jurisdictions have started to draft regulations to oversee the design, deployment, and accountability of AI systems. The EU, for example, has adopted a risk-based framework in the Artificial Intelligence Act, distinguishing between different types of AI applications based on their potential risks and regulating more strictly the use of systems with a higher risk, such as requirements for transparency, human supervision and conformity assessments (European Commission, 2024). The OECD AI Principles are likewise focused on growth, sustainable development and human-centred AI governance, with the core principles being robustness, accountability and transparency (OECD, 2019).

The UNESCO's Ethics of Artificial Intelligence framework builds on this global framework of values, principles and rights by establishing a framework for AI governance rooted in respect for human rights, human dignity, and equality (UNESCO, 2021). Despite these developments, however, global regulatory fragmentation continues to be a significant challenge, with various countries having different approaches to regulation, which leads to inconsistencies in enforcement, compliance and ethical standards from country to country. The chapter therefore explores the theoretical underpinnings, the legal issues, the regulatory landscape and the future of AI governance, and emphasises the importance of flexible and responsive legal systems that will adequately react to the rapid technological advancements and maintain the pillars of justice, accountability and human dignity in a future where AI plays a central role.

1. THEORETICAL FOUNDATIONS OF ARTIFICIAL INTELLIGENCE AND LAW

An understanding of the interaction of Artificial Intelligence (AI) and law must rest on a solid theoretical foundation in both fields, because each has its own logic, but they are becoming increasingly interconnected. Law is a formal system of norms, principles and institutions, which is meant to control the behaviour of humans in society by means of obligation, prohibition and permission. It is based on the assumption that the individual is a rational agent who understands the rules and can be held liable for their conduct according to accepted principles of liability, intent and causation (Hart, 1968).

Legal systems are thus grounded in 'normative expectations of human behaviour' which are supported by enforcement mechanisms that are deployed by courts, regulators and institutions. By contrast, AI is a computational and statistical science about designing a system that works as if it had human intelligence such as reasoning, learning, perception, prediction, and decision making (Russell & Norvig, 2021). AI systems work through the process of algorithms and optimizes outputs based on patterns in data, not on moral considerations or legal knowledge. In the era of big data and machine learning, especially deep learning networks, can find complex correlations and perform high-level cognitive functions like language generation, face recognition and predictive analysis with higher accuracy (Goodfellow et al., 2016).

When these two fields intersect, they raise more complicated issues relating to norms and institutions and the roles of agency, responsibility, autonomy and governance. AI systems are more and more serving as “decision intermediaries” in numerous areas – criminal justice, healthcare, finance, public administration, and others – in which their results have a direct impact on legal rights and obligations (Calo, 2015). This calls into question how exactly AI is viewed, whether it is merely a tool in the hands of humans or an entity with its own influence in socio-technical contexts that impact legal decisions.

The convergence aspect from a jurisprudential point of view is an issue of responsibility, which is how the classical legal theories view it, and which rely on a close link between the intention of people and their legal consequences (Hart, 1968). In the case of AI systems, however, the assumption is overturned by the introduction of algorithmic processes that can produce unexpected results, making it more difficult to make causal attributions and determine liability. (Crawford, 2021) Furthermore, the growing adoption of predictive analytics in governance can be problematic because of the “algorithmic authority” that may arise when the machine's output plays a role in government actions that were once under the control of human minds and bodies (Zuboff, 2019). Furthermore, the adoption of AI within legal frameworks creates governance and organizational challenges, such as transparency, explainability and accountability. Numerous AI models are black boxes, meaning they are not easily explained, even by the AI developer (Pasquale, 2015).

The opacity is counter to core legal concepts like due process and procedural fairness that mandate that people have due notice and a right to challenge decisions that impact on their rights (Wachter et al., 2017). Practical studies also show that the use of AI systems can inadvertently embed and reinforce societal inequalities since they are built on past data that contains structural bias (O'Neil, 2016). This highlights the importance of a system of norms and laws, which goes hand-in-hand with technical design. Finally, the relationship between AI and law is more than just technical and more than just purely theoretical and calls for a reflection on both legal agency and institutional responsibility and on the nature of decision-making in technologically mediated societies.

1.1 Legal Theory and the Concept of Responsibility

The concept of responsibility is fundamental to the concept of legal systems, in that the concept of responsibility presupposes that responsibility and blame can be attached to a rational human agency that has the capacity of intention (men's rea) and action (actus reus). This is because it is a basis for both the criminal responsibility and civil liability regimes, making it easier to be able to show to which specific human conduct and decision making it can be traced that harm has been caused (Hart, 1968). Artificial intelligence (AI) systems, however, make a dent in this schema, by adding non-human actors that can create legally consequential results with no intent of a human at the moment of execution. For instance, in the field of finance, AI can trade stocks and bonds at rapid speeds without needing human intervention or instructions, or in medicine, AI systems can assist with diagnoses by identifying patterns according to probabilities rather than using legal reasoning or explicit instructions. For instance, in finance, AI can make high-frequency trading decisions without the human touch or instructions, or in medicine, AI can aid in diagnosis by recognizing patterns based on probabilities instead of legal reasoning or explicit guidelines. (Calo, 2015; Russell & Norvig, 2021). This will result in a "responsibility gap" where harmful outcomes result, but there is no clear legal subject to blame (Matthias, 2004; Danaher, 2016). Legal systems are now beginning to include distributed responsibility models, such as between data controllers, deployers and developers.

1.2 Artificial Intelligence as an Emerging Legal Actor

Contrary to the traditional doctrinal understanding of AI systems not being legal persons, the growing autonomy of these systems, their capacity to acquire new knowledge and to make decisions have made scholars wonder whether they should be considered as "quasi-agents" in legal systems (Bryson et al., 2017). This discussion arises from the fact that complex systems of AI can perform sophisticated tasks, from real-time trading and autonomous navigation to predictive decision-making, without the constant oversight and direct participation of a human agent, and achieve results that are "functional", but not "moral", like human agency (Crawford, 2021). The instrumentalist perspective is part of legal theory and argues that the creation of AI must be understood as a tool or instrument, like traditional software or machines, which is designed by human beings, operated by human beings, or involved in by institutional actors (Calo, 2015). This view keeps the classical liability structures intact and allows for the blaming always to be put on human actors and not on norms, thus preventing any confusion of norms in blame.

The socio-technical systems perspective, however, challenges this view, suggesting that the responsibility of AI systems is distributed and multifaceted, not confined to a single centre, between people, institutions, datasets and algorithmic processes (Latour, 2005). The perspective outlined above suggests that holding individuals accountable for AI's legal implications is not solely a matter of the individual but also involves recognizing the multifaceted nature of AI lifecycle governance, from data collection to model training, deployment, and post-deployment monitoring. A more controversial and emerging proposition is to give limited legal personality to advanced AI systems, across high autonomy fields like algorithmic trading systems, autonomous vehicles or robotic process automation in critical infrastructure. Those who support the idea say that it will help clarify who is responsible and provide compensation through insurance. This approach is highly controversial, however, as it may undermine foundational legal principles, by reducing human accountability and introducing a "moral hazard", in that responsibility is no longer placed on human decision makers but onto non-sentient systems (European Parliament, 2017; Bryson et al., 2017).

The majority of current legal experts thus do not consider naturalizing AI entities as legal persons, but rather a human accountability structure that is supplemented by rigorous regulation.

1.3 Theories of Technological Determinism and Legal Adaptation

Technology and law can be linked with the two models of socio-legal change, namely, the technological determinism and the legal adaptation theory. In order to understand the relationship between technology and law, it is important to understand the two models of socio-legal change, namely technological determinism and legal adaptation theory. Technological determinism holds that the institutional transformations are a consequence of technological innovations; in other words, the institutional change is more likely to be a response to the technological change, which may have already spread throughout the society (Calo, 2015). From this perspective, AI innovation is not always in line with the legislative process, leading to a regulatory gap and governance disconnect.

In contrast, legal adaptation theory focuses on the ability of technology to self-organise, and the need for laws to be used in advance in terms of anticipatory regulation, institutional design and ethical boundaries set at the design stage (Yeung, 2018). This sort of pressure is particularly palpable in the case of AI governance, where quick progress in algorithm development outpaces the gradual pace of statutory changes. The fundamental legal debate is whether the law should continue to be responsive to technological change, or whether it should become a more active approach to governance, to guide new technologies towards beneficial social outcomes.

1.4 Algorithmic Decision-Making and Legal Rationality

AI systems are increasingly influencing high-stakes decisions, such as judicial risk assessment, parole decisions, insurance underwriting, and screening candidates for employment, that are traditionally made by human judges.AI systems are more involved in high-stakes decisions that are traditionally made by human judges, like parole decisions, insurance underwriting, and screening candidates for jobs.

In the United States, alone, algorithmic tools impact the lives of millions of defendants each year in context of pre-trial and sentencing decisions (Angwin et al., 2016). This poses important questions on algorithmic rationality and its viability with legal reasoning. Legal reasoning is interpretive and context sensitive and is infused with values, which means it is always a balancing process among balancing of rights, statutory interpretation and proportional justice. On the other hand, AI systems are based on statistical inference, pattern recognition and optimization functions based on past data (Goodfellow et al., 2016). This separation is a structural tension – the efficiency and consistency that AI enables does not come with a sense of norms. Therefore, there is a call for "human in the loop" governance to maintain accountability, and procedural justice (Wachter et al., 2017).

1.5 The Role of Data in Legal-AI Systems

However, the key resource of modern AI systems is data; machine learning models require massive amounts of data to recognize patterns, approximate probabilities and make predictions. This is used in software like predictive policing, credit scoring, and risk assessment tools, all of which are sensitive categories that are increasingly being used in legal settings in recent years (O'Neil, 2016). But data is not neutral, it is the result of history, institutional practices and systemic injustice in society. AI models trained on these types of data can replicate or perpetuate patterns of bias, which can lead to concerns about fairness, equality, and procedural justice (Buolamwini & Gebru, 2018). This has created an idea of "datafied law" which refers to a situation in which the decision of a court is driven by computational models instead of normative thinking, calling into question the epistemology of law based on interpretive judicial reasoning (Pasquale, 2015).

1.6 Explainability, Transparency, and Legal Accountability

Explainability is a major theoretical question in AI and law, especially in the case of complex deep learning models, where the internal mechanisms and representations are nonlinear and may not be understood even by the model's creator (Goodfellow et al., 2016).

This opacity poses serious challenges for accountability for the people involved, particularly when they are required to know, challenge or appeal automated decisions made in contexts like credit scoring, job screening, or crime risk assessment. Due process and procedural fairness are closely related to transparency, with a legal system that demands that decisions impacting rights be reasoned and subject to review. Affected people and regulators are unable to challenge or audit the results of algorithms without explainability (Pasquale, 2015). This has spurred the creation of Explainable AI (XAI), whose aim is to create explanations that can be understood by humans. But there is still some debate as to whether post-hoc explanations are legally acceptable or whether inherently interpretable models are needed in the context of high-stakes domains (Wachter et al., 2017).

1.7 Ethical and Normative Foundations of AI Law

Apart from the technical and procedural issues, AI governance is also fundamentally embedded in the philosophical or ethical underpinnings of AI use that influence the legal framework of acceptable AI usages. Utilitarian views focus on maximizing overall social welfare, and sometimes explain the use of AI solely on the basis of efficiency benefits in areas like diagnostics, logistics, and administration in health care (Russell & Norvig, 2021). Deontological approaches focus on doing the right thing, not just on efficiency, even if it is a process that is deemed to be morally wrong because it lacks integrity or does not involve consent or respect for autonomy (Floridi et al., 2018). Rights-based theories also highlight the dignity, privacy and equality before the law of the individual as non-negotiable boundaries on algorithmic governance. Such ethical principles have direct relevance to the design of regulation, in how regulation strikes a balance between the protection of fundamental rights and innovation. In the real world, ethical considerations have been added to the legal requirements for the use of AI by conducting impact assessments, transparency measures and accountability obligations as a way to balance the efficiency of artificial intelligence with constitutional and human rights principles (UNESCO, 2021).

2. LEGAL CHALLENGES OF ARTIFICIAL INTELLIGENCE

The use of artificial intelligence (AI) in social, economic and governmental systems poses a myriad of legal challenges that challenge and challenge existing doctrines and institutional capacities. In parallel, as AI becomes more powerful in terms of its efficiency, predictive accuracy, and ability to automate, it is also challenging fundamental legal principles, including liability, accountability, due process, privacy, and equality before the law, which have been reported to be improved by up to 30-50% in some areas of administrative decision making (OECD, 2019). These are not only technical but also normative challenges that ask to re-think the contours of responsibility and justice in the context of an increasingly automated governance regime (Calo, 2015).

Liability and Attribution of Responsibility

Liability is one of the most pressing legal questions associated with AI, as it is when AI systems cause harm, who is liable? Traditional legal systems rely on specific harmful consequences that are clearly connected to human action and/or negligence. But AI systems add complexity because of their probabilistic and adaptive decision-making processes and the opacity of some of their decisions (Calo, 2015). In collisions involving autonomous vehicles, for instance, the blame could rest with the manufacturer, software developer, data supplier, system integrator or end-users, depending on where the collision occurs. However, reports from the industry indicate that more than 90% of the current road accidents result from human error, but transferring the control to AI systems does not remove, it only shifts, legal risk, which makes it harder to attribute the fault (Crawford, 2021). In another context, such as AI-powered financial trading or healthcare diagnostics, mistakes could be caused by skewed training data, the design of the AI model, or interactions with the deployment environment. This fragmentation creates a multi-actor liability issue which is a challenge to the traditional negligence and strict liability as enshrined in the tort law (Crawford, 2021).

Algorithmic Opacity and the Problem of Explainability

Many of the current AI systems, including the multi-layered neural models used in deep learning, are "black boxes" because of the complexity of their internal decision-making processes, even for the system's developers (Goodfellow et al., 2016). This opacity poses serious problems for legal accountability, particularly in high stakes spaces, where algorithmic deliverables, directly impact rights and obligations. In the legal context, explainability plays a significant role in the procedural fairness and the right to a reasoned decision. The right to understand the basis of an administrative or judicial ruling is usually accorded to the subject of the decision, but it is hard to provide or verify meaningful justification in the case of opaque AI systems (Pasquale, 2015). It also poses difficulties for judicial review, since courts could have trouble determining whether a computational decision is lawful, reasonable, or biased, and in some instances, the complexity of the algorithm would make it impossible for the court to see through to the law (Wachter et al., 2017).

Bias, Discrimination and Algorithmic Inequality

AI systems are learnt from data from the past which can contain structural inequalities that perpetuate or magnify bias in hiring, lending, policing, sentencing, etc. (O'Neil, 2016). Empirical research reveals that performance of commercial facial recognition systems is up to 30% incorrect for darker-skinned female users, but less than 1% incorrect for lighter-skinned male users, thus showing significant and stark demographical differences in performance (Buolamwini & Gebru, 2018). Likewise, predictive policing systems have been found to be biased against communities that are already disproportionately policed, creating a vicious circle of surveillance (Angwin et al., 2016). The results are of great concern under equality and anti-discrimination legislation. Algorithmic discrimination is often indirect and systematic, and any harm that may result from algorithmic discrimination is not necessarily intentional or deliberate, unlike human bias, which can take place in many ways and is not necessarily evident from a legal perspective.

Data Protection and Privacy Concerns

The capacity of AI systems to gather and process vast amounts of data, frequently personal, behavioural, and biometric, introduces substantial privacy, consent, and data protection concerns in today's regulatory landscape, including the GDPR (European Parliament 2016). One of the most critical issues is informed consent, where users often do not have meaningful knowledge of the data collection, processing, or re-use in AI training pipelines. Research has found that, in digital settings, most users accept data practices without reading the terms, which means this is not truly done voluntarily (Acquisti et al., 2015). Furthermore, re-identification methods can render anonymization ineffective; it has been shown that in anonymized data sets more than 80% of people can be re-identified with the help of additional information (Narayanan and Shmatikov, 2008). Purpose limitation principles are further complicated when using secondary data.

Accountability Gaps and Institutional Limitations

The accountability gaps arising from the diffusion of responsibility for oversight and enforcement tasks between different entities involved in the design, deployment, and regulation of AI systems can be particularly problematic. There are a number of regulatory bodies with limited technical expertise to audit intricacies of machine learning systems, and evidence challenges in determining how algorithms work and what caused them to take the decisions that they did (Calo, 2015). Additionally, AI creation is becoming more and more a multi-jurisdictional endeavour, with companies operating in several jurisdictions, which can make it challenging to enforce legal standards in the event of harms transiting across borders (Crawford, 2021). This jurisdictional fragmentation reduces the coherence of the regulatory system and may result in “regulatory arbitrage” by companies taking advantage of weaker systems. This can lead to regulatory inertia if the responsibility for regulating an AI system is also poorly defined, leaving it to operate even if it is deemed to be unsafe or unfair.

Intellectual Property and Ownership Issues

Complex issues in intellectual property (IP) law also arise with the use of AI, including questions of authorship and ownership of AI-generated work. Conventional IP protection relies on the concept of human creativity as the basis of protection, and protection is granted when a work is original, and the author is identifiable. With the advent of generative AI, however, music, visual art, literary works, and even technical inventions can now be created with little human involvement, making the distinction between machine and human creativity increasingly indistinct (Ginsburg & Budiardjo, 2019). There are unresolved legal issues regarding the copyright of AI-generated works and the question of ownership of the works (is it the developer or user or the institution using them). The majority of legal systems today do not recognize AI as an inventor or author of intellectual property per se, leaving the right to it with the humans who create it. Whereas, courts and patent offices in other countries like the EU or the US have repeatedly refused to award patents on AI inventions, thus supporting a doctrine of anthropocentric IP (European Parliament, 2020). But with the quick pace of the developments in generative AI and autonomous innovation systems, this role faces growing threats to traditional legal boundaries and the need for a change in the legal notions of ownership and originality rules.

Criminal Liability and Autonomous Systems

Additionally, AI raises challenges for criminal law, especially in relation to men's rea or intent, the culpable mind of a human actor. Criminal law is also being complicated by AI, particularly with regard to men's rea or intent, the culpable mind of a human actor. This makes it hard to find liability under the traditional criminal notion, which requires intent and action (Hallevy, 2010). In the case of an autonomous drone killing or injuring a person, for instance, the question of responsibility might be spread to the operator, the program or software developer, the manufacturer and/or the institution deploying the drone. Traditionally, criminals are human beings who make decisions based on their operation within boundaries. Traditional criminal law is not suitable for non-human agents that can think for themselves within the boundaries of their operations.

This has sparked continuous discussions around the need for new liability regimes, like strict liability for the use of AI, or vicarious liability for operators, to effectively resolve harms caused by AI.

Procedural Justice and Due Process

Transparency, participation and challenging decisions are essential to procedural fairness, which is one of the foundations of legal systems. Administrative or judicial applications of AI systems might violate these rules if people can't fully comprehend or challenge the results generated by AI systems. Empirical governance research has demonstrated that automated decision systems are now increasingly used in welfare allocation and credit scoring, and that there are few frameworks that offer explanations for these decisions (Pasquale, 2015). If, for example, a welfare benefit or a loan is refused by an AI system, those concerned should be able to get clear explanations and to make an effective appeal. Otherwise, AI-based decision-making may infringe on the due process rights and undermine the standards for administrative justice (Wachter et al., 2017).

Global and Cross-Border Legal Complexity

The scope of an AI system can span multiple jurisdictions, such as developing the system in one country, using data from another country to train the system and then deploying it in a country that is completely different. This transnational architecture presents complex jurisdictional, enforcement and conflict of laws issues, including in relation to cross-border harm cases (Crawford, 2021). The lack of harmonised international AI regulation also makes it harder to enforce regulations properly, as it allows for regulatory arbitrage, with companies exploiting less strong governance environments. This fragmentation has a negative impact on the accountability and on the coherence of the legal order in emerging digital governance systems, scholars note (Calo, 2015). This means that international cooperation is still vital in order to provide effective oversight of AI.

3. REGULATORY AND GOVERNANCE FRAMEWORKS FOR ARTIFICIAL INTELLIGENCE

As artificial intelligence (AI) is more and more integrated into important industries, world efforts to create strong legal and governance structures meant to guarantee safety, transparency, responsibility, and human rights alignment while yet supporting innovation and economic growth have accelerated. According to projections, artificial intelligence could add as much as $15.7 trillion to the world economy by 2030, hence driving regulatory focus on its structural effects (PwC, 2017). But because of how quickly artificial intelligence is developing, how widely it is used across industries, and how complicated cross-border use is, governance still seems challenging. AI systems learn and change often after deployment, unlike conventional technology, therefore static legislative frameworks are inadequate (Yeung, 2018). To handle new hazards efficiently, contemporary AI governance therefore uses hybrid frameworks integrating legal rules, ethical standards, technical standards, and institutional oversight systems.

The Rationale for AI Regulation

The possible effects of artificial intelligence (AI) on basic rights, social fairness, and public safety drive its main reason for regulation. High-stakes judgments in employment, healthcare, education, criminal justice, and financial services, where algorithmic outputs can directly affect life chances and legal results, are increasingly embedded in AI systems. Empirical data reveals major differences caused by algorithmic bias, such as increased misclassification rates in facial recognition systems for some demographics (Buolamwini & Gebru, 2018). Unchecked, artificial intelligence might exacerbate structural inequalities, create fresh damages, or run opaquely to restrict contestability. The "responsibility gap" emphasizes the need for governance since semi-autonomous or autonomous vehicles challenge conventional responsibility assignment mechanisms (Danaher, 2016).

Therefore, regulation is needed to defend human rights and dignity, guarantee responsibility in automated decision-making, advance justice and non-discrimination, improve transparency and explanation, and define safety and dependability criteria.

International rules such the OECD Artificial Intelligence Principles highlight human-centred values and responsibility in AI application (OECD, 2019). Likewise, UNESCO's ethical standards highlight that artificial intelligence systems have to honour human dignity and equality while yet under significant human supervision (UNESCO, 2021). These regulatory goals taken together seek to guarantee that AI development matches legal requirements and society expectations while simultaneously lowering systematic hazards connected with unapproved automation.

Risk-Based Regulatory Models

With related compliance requirements, the risk-based regulatory model, which categories artificial intelligence systems based on the degree of risk they offer for people and society, is among the most often used approaches to artificial intelligence control. The European Union's AI Act, which estimates that over 75% of AI applications fall into minimal or limited-risk categories while just a small percentage are categorized as high-risk but account for most of the regulatory attention (European Commission, 2024), this approach is vital. Strict standards including pre-deployment conformity evaluations, required human supervision, openness documentation, and constant monitoring apply to high-risk systems, those used in biometric identification, judicial decision support, and healthcare diagnosis. Lower-risk systems including recommendation engines and spam filters are given less legal attention to foster creativity while reducing administrative load. This tiered system lets authorities effectively distribute enforcement resources and focus on systems most likely to cause damage. Experts contend that the risk-based approach strikes a practical balance between invention and protection since it guarantees safeguards for crucial uses impacting basic rights while avoiding overregulation of low-impact technologies (Veale & Borgesius, 2021). Therefore, many consider it among the most flexible platforms for modern AI management.

Comparative Global Approaches to AI Governance

Reflecting variations in legal traditions, political systems, and economic priorities, artificial intelligence management differs greatly across countries.

The European Union uses a rights-based, cautious regulatory framework; the United States prefers a sector-specific, innovation-driven approach with sporadic supervision. By contrast, China runs under a state-centric governance system stressing control, security, and algorithmic control (Calo, 2015; Lee, 2018). These differences make it harder for global rules to be consistent and cause worldwide legal fragmentation.

European Union: Rights-Based and Precautionary Approach

Emphasizing basic rights, consumer protection, and ethical compliance under a precautionary governance model, the European Union has implemented one of the most thorough regulatory systems for artificial intelligence. This method gives avoiding damage before deployment first priority, especially in high-risk areas including healthcare and biometric identification. The EU AI Act categorises systems by risk level and places significant responsibilities on high-risk apps, including transparency, human supervision, and conformity evaluations (European Commission, 2024). Many consider it a worldwide standard for rights-based artificial intelligence management (Veale & Borgesius, 2021).

United States: Sectoral and Innovation-Oriented Regulation

On the other hand, the United States uses a dispersed, sector-specific regulatory strategy for artificial intelligence that depends on groups like the Food and Drug Administration and Federal Trade Commission instead of a single federal legislation for artificial intelligence. Though it emphasizes creativity, market adaptability, and private-sector leadership, this approach causes scattered supervision and erratic application across sectors (Calo, 2015).

China: Security-Focused and State-Led Governance

Strong state engagement and centralized management define China's artificial intelligence governance system, which stresses data security, algorithmic responsibility, and alignment with national development goals. This helps China to lead in facial recognition infrastructure by allowing fast implementation of artificial intelligence at scale, especially in smart city and monitoring systems.

However, experts point out problems with state surveillance, privacy, and restricted personal freedom under this paradigm (Lee, 2018; Crawford, 2021).

Emerging Economies

Still in early stages of AI regulation, many underdeveloped nations confront difficulties including little technical know-how, inadequate institutional capacity, and reliance on foreign-developed AI systems. Notwithstanding these difficulties, especially in developing digital economies, there is increasing awareness of the need of local governance systems tackling digital inequality, labour displacement, and data sovereignty (UNESCO, 2021).

Soft Law and Ethical Management

Besides official laws, soft law tools are very important for guiding AI governance. These comprise voluntary codes of behaviour, ethical standards, and technical standards created by professional organizations and global agencies. Given the quick rate of technical development, soft law is especially important in AI regulation since it allows more flexible and adaptive administration that may change along with new risks and uses (Floridi et al., 2018). Ethical systems usually underline ideas like openness, responsibility, justice, privacy, and human supervision. Even if they are non-binding, these guidelines greatly affect business governance policies and sometimes inform the creation of hard legislation like the EU AI Act. These also act as guiding principles for international artificial intelligence governance projects headed by groups including the OECD and UNESCO (UNESCO, 2021; OECD, 2019).

Managerial Mechanisms for Supervision

Good AI control calls for good institutional frameworks that may monitor, implement, and evaluate. These cover data protection agencies, autonomous algorithmic audit organizations, ethics committees, national regulatory bodies with artificial intelligence-specific responsibilities, and international governance bodies for cross-border cooperation. Such frameworks are critical to solve fragmented legislative power and growing artificial intelligence systems' governance deficiencies (OECD, 2019).

A crucial accountability tool, algorithmic auditing lets outside parties assess AI systems for bias, transparency, accuracy, and legal compliance. Research reveal that independent audits greatly reduce the possibility of discriminatory results in high-risk systems, especially in hiring and credit scoring settings, therefore improving public trust and legal control (Raji et al., 2020).

Overseas Collaboration and Standardization

Given the worldwide nature of AI development and implementation, international collaboration is critical as AI systems frequently cross boundaries via cloud infrastructure and worldwide data flows. Emphasizing human rights, openness, and responsibility in artificial intelligence governance, organizations such as the OECD, UNESCO, and the United Nations have released non-binding guidelines (OECD, 2019; UNESCO, 2021). But because of geopolitical rivalry, different legal systems, and competing economic interests among the main AI nations, establishing binding international treaties is still tough. This fragmentation restricts enforcement consistency and impairs world cooperation, therefore making harmonized AI control a continuous international policy issue (Calo, 2015).

Vital Issues in Artificial Intelligence Management

AI regulation still has ongoing difficulties even with a lot of improvement. Many lack enough technical knowledge to evaluate complex machine learning systems, hence regulatory organizations sometimes find technological complexity difficult. Legal systems change much more slowly than fast AI invention cycles, hence regulatory lag is also very important (Calo, 2015). Global fragmentation across countries also produces conflicting standards and enforcement gaps. Furthermore, because AI systems are opaque and large-scale, it is still difficult to carry out effective enforcement; instead, large tech companies greatly affect regulatory design and policy results (Crawford, 2021). These difficulties underline the need of ongoing change and interdisciplinary management.

4. FUTURE DIRECTIONS AND EMERGING ISSUES IN LAW AND ARTIFICIAL INTELLIGENCE

Legal systems are under rising pressure to predict and address new hazards, possibilities, and governance gaps as artificial intelligence develops at a hitherto unheard-of speed. The future of artificial intelligence and law will be determined by proactive legal innovation, interdisciplinary teamwork, and flexible governance frameworks able to answer ongoing technical advancement rather than just reactive legislation. Research show that over 70% of regulations worldwide are still industry-specific and behind AI deployment cycles, therefore spotlighting fundamental governance issues (OECD, 2019). This chapter looks at developing problems influencing AI law, such autonomous decision-making, liability reform, and international legal alignment (Calo, 2015).

Autonomous and Agentic Artificial Intelligence Systems Rising

The rise of very autonomous or "agentic" AI systems able to plan, carry out, and adapt tasks across many fields with little human oversight is among the most important future changes in artificial intelligence regulation. These technologies may dynamically adjust goals unlike present limited artificial intelligence applications, therefore aggravating issues with control, predictability, and lack of human supervision (Russell, 2019). This poses great legal difficulties: Conventional ideas of direct causation and negligence can become inadequate if an AI system starts dangerous acts on its own. Experts contend that liability could have to move toward models of shared accountability that include developers, deployers, and operators all across the artificial intelligence life cycle (Calo, 2015). Strict pre-deployment certification procedures akin to aviation or medicines, whereby safety validation is required before high-risk autonomous systems are released into public settings, may therefore be implemented (OECD, 2019).

AI and the Change of Legal Profession

Artificial intelligence is a revolutionary instrument transforming legal practice itself in addition to a topic of regulation.

AI-driven tools help more and more with things like legal research, contract analysis, predictive litigation analytics, and document automation; studies show that automation can cut document review time in major legal processes by up to 60-70% (Surden, 2014). This change begs important issues about legal professionals' future function. Though it lowers costs and increases efficiency, artificial intelligence also brings with it dangers of over-reliance on automated output, hidden algorithmic mistakes, and less human supervision in difficult legal thinking. Thus, the legal industry will most likely move toward interpretation, strategic judgment, ethical supervision, and human-centred advocacy, so displacing repetitive administrative work (Calo, 2015).

Algorithmic Governance in Government Administration

Reflecting a worldwide change toward "algorithmic governance," governments are using artificial intelligence tools more and more for public administration, including tax enforcement, immigration processing, criminal justice decision support, and welfare distribution. Research show that automating public services will help to increase administrative efficiency and consistency by lowering processing times by 20-40% (OECD, 2019). These systems do, nevertheless, also carry dangers including less openness, less public involvement, and more systematic prejudice in policy application. Algorithmic decision-making in welfare and justice systems has been criticized for limited explainability and accountability, especially when affected people cannot meaningfully challenge outcomes (Pasquale, 2015). Future legal systems will probably call for better protections including required human assessment, open explainability requirements, and algorithmic impact assessments before use in public services (Wachter et al., 2017).

The Growing Importance of Digital Rights

Digital rights are predicted to greatly increase as artificial intelligence pervades daily life and mirrors the rising impact of algorithmic systems on human decision-making. Rising rights debate encompasses data portability, protection against discriminatory algorithmic treatment, human review of high-impact results, algorithmic openness, and explanation of automated decisions.

These rights are increasingly based on data protection systems like the GDPR, which includes safeguards against profiling and automated decision-making (European Parliament, 2016). Researchers contend that such safeguards are necessary to maintain procedural fairness and accountability in algorithmic governance, particularly as artificial intelligence (AI) systems increasingly mediate access to employment, credit, healthcare, and justice (Wachter et al., 2017). Therefore, legal systems might need to more clearly incorporate these digital rights inside constitutional or statutory frameworks to guarantee enforceable protections against algorithmic damage.

AI and the Evolution of Liability Frameworks

AI algorithms that learn and change post-deployment strain traditional liability rules. Future laws could lean toward hybrid responsibility models combining components of product liability, strict liability, and negligence. Risk-based liability is one new idea; it means that liability is assigned according on how much control and risk exposure every actor in the AI lifecycle has. This strategy might assist in resolving the complexity of multi-actor AI environments. Especially in high-impact industries including autonomous vehicles, healthcare, and finance, insurance mechanisms could also help to control AI-related risks even more.

Global Governance and Harmonization's Push

Given the global character of AI development and implementation, future governance would rely more and more on international collaboration and standardization of norms. Regulatory fragmentation without organized structures might cause legal uncertainty, variable protections, and regulatory arbitrage across territories. Estimates show that more than 70% of artificial intelligence systems rely on cross-border data flows, therefore stressing the need of worldwide coordination (OECD, 2019). Possible changes include worldwide AI safety standards, multipolar treaties tackling autonomous weapons and AI warfare, cross-border data governance policies, and international auditing frameworks for high-risk systems. However, geopolitical rivalry among significant technical countries still constrains the viability of totally harmonized worldwide legislation (Crawford, 2021).

Ethically AI and Value Alignment Issues

A great future difficulty is making sure artificial intelligence systems match human values, legal standards, and ethical standards—a difficulty sometimes known as "value alignment." Matching machine goals with human intention gets more difficult as AI systems grow more autonomous and complicated (Russell, 2019). Various civilizations give different importance to privacy, autonomy, justice, and security, therefore universally implemented artificial intelligence systems could run against contradictory legal expectations across nations. This begs issues with ethical pluralism and government consistency. Thus, future legislation could call for culturally sensitive rules that strike a balance between local moral standards and worldwide minimum human rights and safety safeguards (UNESCO, 2021).

Artificial Intelligence, Work, and Sociological Change

AI-driven automation is anticipated to fundamentally alter labour markets; projections show up to 40% of present employment may be exposed to automation hazards in the next decades, especially in routine cognitive and manual chores (OECD, 2019). This brings up important legal and political questions about labour rights, social security, and fair wealth redistribution. Potential legislative answers could be taxes on AI, universal basic income trials, required workforce reskilling initiatives, and more labour safeguards for algorithm-managed employees in platform economies. These actions seek to reduce displacement risks and guarantee inclusive economic changes in more and more automated societies (Brynjolfsson & McAfee, 2014).

Explainable and Trustworthy Artificial Intelligence

Future artificial intelligence management will still centre on explainability as ever more sophisticated machine learning systems defy human interpretation. Maintaining public confidence, procedural justice, and legal responsibility depends on making sure that algorithmic conclusions are clear (Goodfellow et al., 2016). Research reveals a major drop in user confidence in automated systems, especially in critical fields like healthcare and criminal justice, due to opacity (Pasquale, 2015).

Therefore, forthcoming rules may demand "auditability by design," therefore guaranteeing structural building of AI systems to allow for regulatory scrutiny, traceability, and compliance checking throughout their lifecycle. Reliable artificial intelligence is increasingly being codified as a legal requirement rather than a moral goal, as seen in new OECD and EU legislation (OECD, 2019; European Commission, 2024).

CONCLUSION

One of the most important technical developments in contemporary history, artificial intelligence has major effects on legal theory, legal practice, and government systems. This chapter has shown how artificial intelligence challenges fundamental legal ideas as accountability, responsibility, openness, and justice while also providing strong tools to improve legal research output, administrative decision-making, and judicial efficiency (Russell & Norvig, 2021). Empirical research show that AI-assisted legal processes might save case analysis and document review time by as much as 60%, therefore transforming institutional capacity and professional legal practice (Surden, 2014).

Theoretical study reveals that artificial intelligence challenges conventional beliefs about human agency and calls for fresh frameworks of distributed responsibility and algorithmic accountability. Legal challenges call attention to ongoing problems including algorithmic bias, transparency, data security concerns, and cross-border enforcement difficulty (Calo, 2015). Regulatory frameworks show a divided worldwide scene whereby nations embrace varied governance systems ranging from China's state-centric system to the United States' sectoral approach and the EU's rights-based artificial intelligence Act. Rising concerns further show that law has to always change to match ever more independent and embedded systems able of self-learning and decision-making outside of human influence (Crawford, 2021). The main lesson is that law in the age of artificial intelligence has to be flexible, multidisciplinary, and forward-looking. Legal systems have to actively influence artificial intelligence development to guarantee alignment with democratic values, human rights, and ideas of justice instead of fighting technical change.

To create strong governance frameworks for an AI-driven society, technologists, legal experts, legislators, and ethicists must constantly work together.

REFERENCES

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509-514. https://doi.org/10.1126/science.aaa1465

Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). Machine bias. *ProPublica*. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

Bryson, J. J., Diamantis, M. E., & Grant, T. D. (2017). Of, for, and by the people: The legal lacuna of synthetic persons. *Artificial Intelligence and Law, 25*(3), 273-291. https://doi.org/10.1007/s10506-017-9214-9

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research, 81*, 1-15. http://proceedings.mlr.press/v81/buolamwini18a.html

Calo, R. (2015). Robotics and the lessons of cyberlaw. *California Law Review, 103*(3), 513-563. https://doi.org/10.15779/Z38H41D

Crawford, K. (2021). *Atlas of AI: Power, politics, and the planetary costs of artificial intelligence*. Yale University Press. https://yalebooks.yale.edu/book/9780300209570/atlas-of-ai/

Danaher, J. (2016). The threat of algocracy. *Philosophy & Technology, 29*(3), 245-268. https://doi.org/10.1007/s13347-015-0211-7

European Commission. (2024). *Artificial Intelligence Act*. https://eur-lex.europa.eu

European Parliament. (2016). *General Data Protection Regulation (GDPR) (EU) 2016/679*. https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Parliament. (2017). *European Parliament resolution on civil law rules on robotics (2015/2103(INL))*. https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html

European Parliament. (2020). *Intellectual property rights for the development of artificial intelligence technologies*. https://www.europarl.europa.eu

Floridi, L., et al. (2018). AI4People: An ethical framework for a good AI society. *Minds and Machines, 28*, 689-707. https://doi.org/10.1007/s11023-018-9482-5

Ginsburg, J. C., & Budiardjo, L. A. (2019). Authors and machines. *Columbia Law Review, 119*, 2219-2296. https://columbialawreview.org/content/authors-and-machines/

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press. https://www.deeplearningbook.org/

Hallevy, G. (2010). The criminal liability of artificial intelligence entities. *Alabama Law Review, 64*, 545-562. https://heinonline.org

Hart, H. L. A. (1968). *Punishment and responsibility: Essays in the philosophy of law*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199534777.001.0001

Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory*. Oxford University Press. https://global.oup.com

Lee, K.-F. (2018). *AI superpowers: China, Silicon Valley, and the new world order*. Houghton Mifflin Harcourt. https://www.hmhbooks.com

Matthias, A. (2004). The responsibility gap: Ascribing responsibility for the actions of learning automata. *Ethics and Information Technology, 6*, 175-183. https://doi.org/10.1007/s10676-004-3422-1

Narayanan, A., & Shmatikov, V. (2008). Robust de-anonymization of large sparse datasets. *IEEE Symposium on Security and Privacy*, 111-125. https://doi.org/10.1109/SP.2008.33

O'Neil, C. (2016). *Weapons of math destruction*. Crown Publishing. https://www.penguinrandomhouse.com

OECD. (2019). *OECD principles on artificial intelligence*. https://oecd.ai/en/ai-principles

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press. https://www.hup.harvard.edu/books/9780674368279/the-black-box-society

PwC. (2017). *Sizing the prize: What's the real value of AI for your business and how can you capitalise?* https://www.pwc.com

Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., Smith-Loud, J., Theron, D., & Barnes, P. (2020). Closing the AI accountability gap. *FAT* '20, 33-44. https://doi.org/10.1145/3351095.3372873

Russell, S. (2019). *Human compatible: Artificial intelligence and the problem of control*. Viking. https://www.penguinrandomhouse.com

Russell, S., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson. https://aima.cs.berkeley.edu/

Selbst, A. D., & Barocas, S. (2018). The intuitive appeal of explainable machines. *Fordham Law Review, 87*, 1085-1139. https://fordhamlawreview.org

Surden, H. (2014). Machine learning and law. *Washington Law Review, 89*, 87-114. https://digitalcommons.law.uw.edu

UNESCO. (2021). *Recommendation on the ethics of artificial intelligence*. https://unesco.org/en/artificial-intelligence/recommendation-ethics

Veale, M., & Borgesius, F. Z. (2021). Demystifying the draft EU Artificial Intelligence Act. *Computer Law & Security Review, 42*, 105582. https://doi.org/10.1016/j.clsr.2021.105582

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation does not exist in the GDPR. *International Data Privacy Law, 7*(2), 76-99. https://doi.org/10.1093/idpl/ipx005

Waldron, J. (2016). *The rule of law and the measure of property*. Cambridge University Press. https://doi.org/10.1017/CBO9781139136914

Yeung, K. (2018). Algorithmic regulation: A critical assessment. *Regulation & Governance, 12*(4), 505-523. https://doi.org/10.1111/rego.12158

Zuboff, S. (2019). *The age of surveillance capitalism*. PublicAffairs. https://www.publicaffairsbooks.com

CHAPTER 2
PROTECTION OF PERSONAL IMAGE AS A FORM OF PERSONAL DATA IN CYBERSPACE: AN APPROACH FROM PERSONALITY RIGHTS AND THE RIGHT TO DATA CONTROL

Hoang Le BUU[1]
Nguyen Huynh Ngoc ANH[2]
Vo Thi TAM[3]
Le Nguyen Thao UYEN[4]

[1]Thu Dau Mot University, buuhl@tdmu.edu.vn, ORCID ID: 0009-0004-1854-1064
[2]Thu Dau Mot University, anhnhn@tdmu.edu.vn
[3]Van Lang University, tam.vo@vlu.edu.vn
[4]Thai Binh Duong University, uyen.lnt@tbd.edu.vn

INTRODUCTION

For a long time, personal images have been recognized as one of the fundamental personality attributes, intrinsically linked to the honour, dignity and self-determination of every individual. In the traditional legal order, the protection of personal images primarily revolved around the issue of consent to the taking, retention and publication of images, considered in the context of direct civil relationships and tangible media. However, the development of the digital environment has fundamentally transformed both the nature and scope of acts relating to personal images, thereby raising new legal questions that the traditional regulatory framework is no longer capable of addressing adequately.

In cyberspace, a personal image does not exist merely as a single photograph or video, but is digitised into data, stored on servers, indexed by search engines, analysed by facial recognition algorithms, combined with other sources of information to construct personal profiles, and exploited for commercial purposes or social control. An individual's image can be copied an unlimited number of times, disseminated across multiple platforms, edited or fabricated through deepfake technology, or incorporated into training datasets for artificial intelligence (AI) models. In many cases, the person whose image is used is completely unaware of, and unable to control, what is happening to that image.

This situation calls for a re-conceptualisation of the legal status of personal images. Images in the digital environment are not merely objects of personality rights in the traditional sense; they also constitute a form of personal data capable of identifying individuals and are therefore subject to personal data protection law. These two legal frameworks do not exclude each other; on the contrary, they are complementary and must be applied concurrently in order to provide full protection for individuals against increasingly diverse risks in cyberspace.

This chapter analyses personal images from the perspective of personality rights and data control rights, clarifies the intersection and mutual reinforcement between these two approaches, assesses the current state of Vietnamese law, and proposes directions for legal reform in the face of emerging challenges posed by digital technologies.

1. PERSONAL IMAGES BETWEEN PERSONALITY RIGHTS AND PERSONAL DATA

1.1 The Legal Nature of Personal Images as a Personality Right

The right to personal images belongs to the group of non-pecuniary personality rights, which are intrinsically linked to each individual's personality and are non-transferable. The legal nature of this right derives from the organic relationship between an image and personal identity: an image is not only external information about a person's physical appearance but also a visual manifestation of personality, a factor through which the individual is identified and associated with honour, dignity and reputation in social relations (Civil Code of Vietnam 2015, Article 32). Because images are so closely bound up with personal identity, the ability to control how one's image is used and disclosed to the public is a manifestation of personal autonomy.

In legal scholarship, the right to images is often analysed in connection with at least three closely related groups of personality rights. First is the right to privacy, under which every individual has the right to control what information about themselves is placed in the public sphere; an image is one such piece of information, and the dissemination of images against the will of the person concerned may constitute an intrusion into privacy (Solove, 2008). Second is the right to honour, dignity and reputation, since images that are edited or placed in a misleading context may seriously damage the reputation of the person depicted. Third is the right to informational self-determination in a broader sense, concerning an individual's ability to decide on their own public presence and on the ways in which others access information about them (Westin, 1967).

This interconnectedness makes the right to personal images a complex, composite right. On the one hand, it protects purely moral interests when images are used in ways that are insulting, defamatory or cause psychological harm. On the other hand, it protects personality-based pecuniary interests where images are commercially exploited without the consent of the person concerned, as recognized in the doctrine of the right of publicity in United States law and a number of other legal systems (Brunskell, 2022).

Although Vietnamese law has not developed the notion of a separate "right of publicity", the provisions of the 2015 Civil Code have tentatively acknowledged the commercial interests attached to images by requiring the consent of the individual and their legal representative in cases where images are used for commercial purposes. It should be emphasised that the personality right to images is not absolute. It always exists in tension with competing rights and interests, in particular freedom of expression, freedom of the press, the right of access to information and the public interest. Where the images of public figures or historical personalities are concerned, the scope of personality rights is significantly narrowed. Nevertheless, even in such cases, personality rights establish a minimum threshold of protection that no one may overstep: no one is permitted to use the image of another in a manner that affronts human dignity or causes harm that cannot be justified by the public interest.

1.2 The Transformation of Personal Images into Data in the Digital Environment

The digital environment alters the mode of existence of personal images in ways that the traditional regulatory framework did not anticipate. Once an image is digitised, it is no longer a physical object existing in a specific place but becomes a string of data that can be replicated infinitely, stored on multiple servers in different countries, transmitted instantaneously through digital networks and processed by automated systems without human intervention. Particularly significant is the biometric identifiability of images. The human face is a special type of biometric data, as it is both personal information and a unique identifier that allows AI systems to recognise, track and profile individuals without requiring them to disclose any information themselves. The European Union's General Data Protection Regulation (GDPR) defines "biometric data" as personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person which allow or confirm the unique identification of that natural person (Regulation (EU) 2016/679, Article 4(14)). Under this definition, digital portrait photographs, when fed into facial recognition systems, may constitute biometric data and are therefore classified as sensitive data subject to a higher level of protection.

Personal images in the digital environment also exhibit five distinctive features compared to images in the traditional environment. First is the ability to copy and disseminate without limit, which means that once an image has been leaked, it is almost impossible to retrieve completely. Second is the potential for re-contextualisation, where images are cropped, spliced, placed in new contexts or combined with other information to create a meaning entirely different from their original meaning. Third is the ability to combine and re-identify, where images are aggregated with other data sources (geolocation, behavioural habits, search histories) to create detailed personal profiles. Fourth is digital persistence, whereby images can remain on platforms indefinitely even after the user deletes the original. Fifth is the capacity for automated processing, where algorithms can analyse millions of images to detect faces, emotions, behaviours or identifying characteristics without any human reviewing each image (Solove & Hartzog, 2022).

These features make personal images in the digital environment a form of personal data in the technical legal sense: information relating to an identified or identifiable individual. Vietnam's Decree No. 13/2023/ND-CP defines personal data as information in the form of symbols, writing, digits, images, sounds or similar forms in the electronic environment that is associated with a specific human being or helps identify a specific human being (Decree No. 13/2023/ND-CP, Article 2). This definition clearly encompasses images as a form of personal data, thereby placing images simultaneously under the regulation of civil law on personality rights and of personal data protection law.

2. PROTECTING PERSONAL IMAGES IN CYBERSPACE FROM THE PERSPECTIVE OF DATA CONTROL RIGHTS

2.1 The Intersection between Personality Rights and Data Control Rights

The right to control personal data, also referred to as the right to informational self-determination, is rooted in a legal-philosophical premise similar to that of personality rights: individuals must be able to control information about themselves because such information is inseparable from their personality and autonomy in social life.

The Federal Constitutional Court of Germany developed this doctrine in its 1983 census judgment (Volkszählungsurteil), holding that the right to informational self-determination is part of the general personality right protected by the constitution (Bundesverfassungsgericht, 1983). From this theoretical foundation, it is evident that personality rights and data control rights are not entirely independent but share common roots in the doctrine of personal autonomy.

However, the two legal frameworks differ in their methods of protection and scope of regulation. Personality rights protect individuals against specific infringements such as the unauthorised use of images, defamation or intrusions into private life, primarily through mechanisms for damages and orders to cease the infringing acts. By contrast, personal data protection law establishes a more preventive and structural set of obligations: data controllers must have a valid legal basis before processing data, must comply with principles such as purpose limitation, data minimisation and security, and must ensure the effective exercise of data subject rights. This system does not wait for infringements to occur before intervening but sets prior conditions governing the entire data-processing lifecycle (Bygrave, 2014).

With respect to personal images in cyberspace, the combination of these two frameworks creates a multi-layered protective regime. Personality rights protect against direct infringements and acts that harm honour, dignity or private life. Data control rights protect against the collection, storage, analysis and transfer of images through automated processes without consent or another valid legal basis. In some situations, either framework alone is sufficient, but in many specific circumstances of the digital environment, such as facial recognition in surveillance systems or the use of images to train AI, both frameworks need to be applied simultaneously.

2.2 Data Subject Rights as Applied to Personal Images

Once personal images are recognised as personal data, the subjects of those images enjoy the full range of rights conferred on data subjects under personal data protection law. These rights provide an active and continuous control mechanism that is qualitatively different from the reactive protection offered by traditional civil law.

The right to be informed requires data controllers to notify individuals about the collection and use of their images, the purposes of processing, the retention period and the identity of the controller. This is a precondition for consent to have legal validity, since consent given without adequate information cannot be considered genuinely voluntary. The right of access entitles individuals to request information about where and how their images are being stored and processed. The right to erasure, or the "right to be forgotten", allows individuals to request the deletion of their images in certain circumstances, particularly where the processing purpose has expired or consent has been withdrawn. Article 17 GDPR provides for this right on eight grounds for erasure, including the withdrawal of consent where there is no other legal basis for continued processing (Regulation (EU) 2016/679, Article 17).

The right to restriction of processing enables individuals to request a temporary suspension of processing while disputes over the accuracy of data or the legal basis for processing are being resolved. The right to object allows individuals to refuse certain forms of processing, particularly for direct marketing or profiling purposes. Equally important is the right to withdraw consent at any time without having to provide reasons, with such withdrawal not affecting the lawfulness of processing carried out before the withdrawal but terminating all subsequent processing based on that consent.

For personal images, the right to withdraw consent has particular significance. In the digital environment, consent is often expressed through the act of posting images on social networks or accepting the platform's terms of use. However, the fact that a person posted an image in the past does not mean that they consent indefinitely to all subsequent uses of that image, especially uses that they could not have foreseen at the time of posting. The rights to withdraw consent and to request erasure are legal tools that enable individuals to regain control in such situations, even though the practical enforcement of these rights still faces considerable technical and legal obstacles.

2.3 Responsibilities of Image Data Controllers and Processors

When personal images are addressed from the perspective of data protection, legal responsibility arises not only for the direct infringer but for all actors involved in the data-processing chain.

The data controller is the entity that determines the purposes and means of processing and bears primary responsibility for ensuring that all processing activities comply with the law. The data processor processes data on behalf of the controller and is responsible for data security within the scope of its assigned tasks.

In the context of personal images on digital platforms, this distinction is not always clear. A social media platform is, to some extent, a controller, as it provides the space where users upload images, yet it also supplies the technical infrastructure for third-party developers to process image data, in which case it may act as a processor or joint controller depending on the specific service. This complexity requires the law to establish clear rules for allocating responsibility and to recognise joint and several liability where multiple actors participate in image processing.

3. VIETNAMESE LAW ON THE PROTECTION OF PERSONAL IMAGES AS A FORM OF PERSONAL DATA

3.1 Provisions of the 2015 Civil Code

The 2015 Civil Code is the foundational legal instrument regulating the right to personal images in Vietnam, enshrined in Article 32. This provision sets out a basic principle: the use of an individual's image must be consented to by that person; images may be used without consent only for the sake of the national, ethnic or public interest; for the use of images for commercial purposes, the consent of the person concerned is required and remuneration may be paid as agreed. The Code also recognises the right to private life, personal secrets and family secrets in Article 38, under which all information relating to private life, personal secrets and family secrets is protected by law, and the collection, retention, use and disclosure of information relating to private life must be consented to by the person concerned.

From the perspective of protecting personal images in the digital environment, Article 32 of the 2015 Civil Code has foundational value but reveals certain limitations. First, the provision uses general language and does not provide adequate legal-technical mechanisms to deal with specific situations of the digital environment such as re-posting, algorithmic processing or facial recognition.

Second, the criterion of "public interest" as an exception to the requirement of consent has not been concretised, leaving room for arbitrary expansive interpretation, particularly where personal images are used under the guise of journalism, media or propaganda. Third, the civil-law framework for damages for infringements of the right to images requires victims to prove actual harm, which is very difficult in many cases of unauthorised use of images online, where the harm is mainly moral and difficult to quantify.

Article 38 of the 2015 Civil Code on private life has a broader scope of regulation and may be invoked to protect images in a number of situations not covered by Article 32, such as images depicting personal activities in private spaces that are disclosed without consent. However, both provisions operate according to a reactive protection model: the law intervenes after the violation has occurred and does not establish proactive compliance obligations for organisations that process images on a large scale.

3.2 Decree No. 13/2023/ND-CP and the Personal Data Protection Regime

Decree No. 13/2023/ND-CP on personal data protection is Vietnam's first specialised regulatory instrument in this field and marks an important step in building a legal framework for data control rights. The Decree recognises personal images as a basic form of personal data (Article 2(1)), and identifies "sensitive personal data" as including biometric data (Article 2(4)), which may cover facial images when processed by recognition systems.

The Decree sets out principles for personal data processing, including processing only for the purposes notified, ensuring accuracy and currency, limiting retention periods and ensuring data security. With regard to consent, the Decree requires that consent be given clearly, voluntarily, specifically and in an informed manner, and it recognises the right to withdraw consent (Article 9). Data subjects are granted rights including the right to know, the right to consent, the right of access, the right to withdraw consent, the right to erasure, the right to restriction of processing, the right to data provision, the right to object and the right to lodge complaints (Articles 9–20). However, when evaluated specifically from the perspective of protecting personal images, the Decree reveals several notable gaps.

First, it lacks specific provisions on the processing of personal images in special contexts such as facial recognition in public spaces, the use of images for AI training, or the exploitation of images for targeted online advertising. Second, the criteria for distinguishing between ordinary images and biometric images are not clearly defined, leading to legal uncertainty about the level of protection applicable. Third, the mechanisms for enforcing data subject rights, particularly the rights to erasure and restriction of processing, lack detailed procedures and clear time limits for handling requests. Fourth, the responsibilities of digital platforms as controllers or processors of image data are not regulated strictly enough, especially with respect to cross-border platforms.

3.3 Related Provisions and Legal Gaps

In addition to the 2015 Civil Code and Decree No. 13/2023, personal images are also regulated by a number of other legal instruments. The 2018 Cybersecurity Law provides for the protection of personal information in cyberspace and imposes obligations on operators of information systems, but its primary focus is on national security and it lacks the detail needed to address civil issues arising from unauthorised uses of images (Cybersecurity Law 2018). The 2012 Law on Advertising requires consent for the use of personal images in commercial advertising, yet it does not specifically regulate digital advertising or algorithmically personalised advertising. Regarding children, the 2016 Law on Children requires the protection of children's personal information and prohibits the disclosure of information that harms children, but it contains no detailed provisions on the processing of children's images in the digital environment, including content posted by parents themselves (sharenting). Overall, the current Vietnamese legal framework regulates personal images in a fragmented structure: personality rights are provided for in civil law, data protection in a specialised decree, cybersecurity in a specific law, and advertising in sector-specific legislation. This fragmentation produces two fundamental problems. First is the lack of conceptual and standard consistency, for example the criteria for "valid consent" are not harmonised across instruments.

Second is the absence of a lead authority with comprehensive jurisdiction to handle disputes concerning personal images, forcing victims to pursue multiple complaint channels with uncertain outcomes.

4. LEGAL ISSUES RAISED AND PROPOSALS FOR IMPROVING VIETNAMESE LAW

4.1 Consent and the Boundaries between Competing Rights

Consent lies at the core of the protection of personal images in both legal frameworks: personality rights require consent for the use of images, and data protection law requires consent (or another legal basis) for data processing. In the digital environment, however, the concept of consent faces serious challenges in terms of substantive validity. Common forms of consent on digital platforms, such as clicking to accept terms of service running to thousands of words, or treating the posting of images on social networks as consent to the platform's entire data policy, can hardly be regarded as genuinely informed and voluntary consent in the sense demanded by law (Nissenbaum, 2010).

This challenge is further complicated once images have been made public online. Some argue that by posting images on social networks, individuals relinquish part of their expectation of privacy in those images. If interpreted too broadly, this view risks legitimising any re-use of publicly available images without additional consent. Nissenbaum's theory of "contextual integrity" (2010), however, argues that a person's decision to share images in a particular context does not imply consent to all other uses of those images in different contexts; information flows are only appropriate when they comply with the norms of the original social context. Applied to images, photographs posted on a person's private profile cannot automatically be used in commercial advertising or for AI training. Alongside issues of consent is the boundary between the right to images and freedom of expression and of the press. Where personal images relate to matters of public interest, such as images of officials performing public duties or images documenting events of historical significance, personality rights must give way to some extent to the public's right to information. However, this boundary is unclear and frequently contested, particularly where images of public figures are used in political commentary, artistic works or investigative reporting.

Vietnamese law has yet to develop clear criteria for delimiting this boundary, resulting in inconsistent application.

4.2 Commercial Exploitation and Facial Recognition Technology

The commercial exploitation of personal images is among the most salient legal issues in the platform economy. Personal images have commercial value not only when used directly in advertising but also when included in datasets to train AI models that recognise facial features, emotions or consumer behaviour. In many cases, the individuals concerned receive no compensation and may be unaware that their images are being exploited commercially. Facial recognition technology presents particularly serious legal challenges. Unlike many other forms of data, a person's face is a unique identifier that is practically impossible to change, which means that once facial data are collected and incorporated into databases, the individual cannot simply "change their password" or erase their digital identity. The deployment of facial recognition systems in public spaces without notice and consent constitutes a form of mass collection of biometric data, infringing both personality rights and data control rights. The European Union Agency for Fundamental Rights (FRA) has observed that facial recognition systems in public spaces risk producing a chilling effect on the rights to freedom of movement, assembly and expression, even when they are not deployed with the direct aim of surveilling those rights (FRA, 2019). Vietnamese law does not yet contain specific provisions on facial recognition. Decree 13/2023 refers to biometric data as a sub-category of sensitive data but does not establish protective measures commensurate with the risks of this technology, in particular by failing to mandate data protection impact assessments, to limit permissible purposes, or to set out special control procedures.

4.3 Deepfake, AI and Fabricated Images

Deepfake technology, which uses AI to create highly realistic fabricated images and videos of real persons, introduces a fundamentally new type of legal risk: the infringing image is not only a real image misused, but an artificial image generated based on the person's facial features.

In theoretical terms, deepfakes simultaneously infringe multiple rights: the right to images (through the use of facial characteristics without consent), the rights to honour and dignity (especially where deepfakes are offensive or reputationally damaging), the right to privacy (where deepfakes depict intimate or sexual content without consent), and potentially the right to data protection (where deepfake creation involves processing biometric data).

At present, Vietnamese law contains no explicit provisions on deepfakes. The creation and dissemination of deepfakes may be addressed under existing rules on defamation (Civil Code 2015, Article 34), false information in cyberspace (Decree No. 15/2020/ND-CP, Article 101), or intrusions into privacy, but these provisions were not designed with deepfake technology in mind and therefore reveal important gaps regarding the definition of infringing acts, levels of sanctions and emergency response procedures. International legislative trends are moving towards criminalising non-consensual intimate deepfakes, as the United Kingdom has done since early 2026 (DLA Piper, 2026), while also imposing prompt takedown obligations on digital platforms.

4.4 The Right to Removal, Compensation for Harm and Emergency Protection Mechanisms

One of the most notable gaps in current Vietnamese law is the absence of rapid and effective mechanisms for image removal. When personal images are disseminated unlawfully online, every passing hour increases the likelihood that they will spread to additional platforms and become difficult to retrieve. Ordinary complaint and civil litigation procedures, which typically take several months to resolve, are entirely incompatible with the speed of information dissemination in the digital environment. The law therefore needs to establish an emergency takedown mechanism under which platforms are obliged to handle requests within a very short timeframe (for example, 24 to 48 hours) in cases involving content that poses a serious risk of harm, such as non-consensual intimate deepfakes, images of individuals in private situations or images of children. With regard to compensation, Vietnamese civil law in principle allows for recovery of both pecuniary and non-pecuniary damage.

However, the provisions on the grounds and amounts of compensation for non-pecuniary damage caused by infringements of the right to images remain general and lack specific quantification criteria, resulting in awards that are typically very low and insufficiently deterrent in practice. Adopting a model of statutory damages, as found in some jurisdictions, whereby victims may claim a predetermined range of compensation without proving actual loss, is a promising approach to enhancing the effectiveness of protection.

4.5 Responsibilities of Digital Platforms and Directions for Reform

Digital platforms, as intermediaries between users and the online community, play a decisive role in whether personal images are protected or infringed. The traditional "safe harbour" mechanism, which immunises platforms from liability for user-generated content, is increasingly being questioned, especially as platforms actively use algorithms to distribute, recommend and monetise content, including personal images. When platforms are no longer merely passive conduits but active participants in processing and exploiting image data, the rationale for complete immunity becomes less convincing.

On this basis, several key directions can be identified for improving Vietnamese law on the protection of personal images. The first is to clarify the dual legal status of personal images by explicitly recognising in law that personal images are simultaneously objects of personality rights and a type of personal data, and to construct a combined protective mechanism reflecting both perspectives. The second is to specify requirements for valid consent in the digital environment, including criteria for valid consent, situations in which implied consent is unacceptable, and clear obligations to provide notice. The third is to adopt specific regulations on high-risk technologies, including facial recognition, deepfakes and AI-based image processing, setting conditions for lawful use and establishing oversight mechanisms. The fourth is to strengthen the responsibilities of digital platforms, including obligations of emergency takedown, transparency regarding image data processing, and liability for failure to implement necessary protective measures.

The fifth is to improve the regime of compensation and emergency measures, particularly by developing a statutory floor for non-pecuniary damages with sufficient deterrent effect and expediting procedures for interim emergency measures in cases involving images. The sixth is to establish an authority or coordination mechanism with comprehensive jurisdiction to handle disputes and supervise compliance in relation to the protection of personal images in cyberspace, thereby overcoming the current fragmentation of competence.

CONCLUSION

Personal images in the digital environment have a distinctive legal character that traditional models do not fully capture. They are at once expressions of personality and human dignity, falling within the scope of personality rights, and digital data capable of identifying individuals, being processed automatically and exploited for multiple purposes, thereby falling within the ambit of personal data protection law. These two dimensions of protection do not replace each other but are complementary: personality rights provide a foundation grounded in human dignity and personal autonomy, while data control rights provide legal-technical tools for managing the data-processing lifecycle in a proactive and systematic manner.

Vietnamese law has recognised both protective frameworks through the 2015 Civil Code and Decree No. 13/2023/ND-CP, yet the intersection between them has not been developed into a coherent and systematic whole. Provisions remain fragmented, lack specific criteria and have not kept pace with the development of new technologies such as facial recognition, deepfakes and generative AI. This is not merely a technical legislative gap but also a matter of theoretical depth: the law must first construct a consistent conception of the legal status of personal images before it can design effective protective mechanisms. Improving the law in this field requires an integrated approach that combines personality-rights thinking with data-governance thinking. It is neither possible to protect personal images in the digital environment solely by extending traditional civil-law provisions, nor sufficient to rely only on technical rules on data processing while neglecting the personality dimension of the right.

A robust legal framework must place the human being, as a subject endowed with dignity and self-determination, at the centre of all processes involving the processing of images in the digital environment.

REFERENCES

Brunskell, J. (2022). The evolving property right of personal image [Doctoral dissertation, Queen Mary University of London]. QMRO Repository.

Bundesverfassungsgericht [Federal Constitutional Court of Germany]. (1983). Volkszählungsurteil [Census Act Judgment], BVerfGE 65, 1.

Bui Thi Thanh Hang. (2021). The right to personal image under Vietnamese civil law. Journal of Legal Studies, (5), 15–28.

Bygrave, L. A. (2014). Data privacy law: An international perspective. Oxford University Press.

Government. (2020). Decree No. 15/2020/ND-CP dated 3 February 2020 on administrative penalties in the fields of postal services, telecommunications, radio frequencies, information technology, and electronic transactions.

Government. (2023). Decree No. 13/2023/ND-CP dated 17 April 2023 on personal data protection.

Council of Europe. (2021). Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data: Guidelines on facial recognition (T-PD-BUR(2020)09rev5). Council of Europe Publishing.

DLA Piper. (2026, April 8). How the law is catching up with AI "deepfakes". https://www.dlapiper.com/insights/topics/algorithm-to-advantage/how-the-law-is-catching-up-with-ai-deepfakes

Dunn, S. (2024). Legal definitions of intimate images in the age of sexual deepfakes and generative AI. McGill Law Journal, 69(1), 1–45. https://lawjournal.mcgill.ca/article/legal-definitions-of-intimate-images-in-the-age-of-sexual-deepfakes-and-generative-ai/

European Data Protection Board. (2020). Guidelines 3/2019 on processing of personal data through video devices (Version 2.0). https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en

European Union Agency for Fundamental Rights. (2019). Facial recognition technology: Fundamental rights considerations in the context of law enforcement. Publications Office of the European Union.

https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law

Georgiades, A. (2021). Protection of personal images on the internet. IDEA: The Law Review of the Franklin Pierce Center for Intellectual Property, 61(2), 1–45.

Grynbaum, T., & Treisman, R. (2022). Image rights in the digital universe. Journal of Intellectual Property Law & Practice, 17(7), 551–561. https://doi.org/10.1093/jiplp/jpac047

Le Dinh Nghi. (2020). Personal rights in Vietnamese civil law: Some theoretical and practical issues. Journal of Legislative Studies, (12), 3–14.

Mendis, D., & Lim, D. (2021). Protecting image rights in the face of digitalization: A United States and European analysis. The Journal of World Intellectual Property, 24(3–4), 1–20. https://doi.org/10.1111/jwip.12194

Nguyen Van Cu, & Tran Thi Hue. (Eds.). (2017). Scientific commentary on the 2015 Civil Code of the Socialist Republic of Vietnam. People's Public Security Publishing House.

Nissenbaum, H. (2010). Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.

National Assembly. (2012). Law on Advertising 2012, Law No. 16/2012/QH13, promulgated on 21 June 2012.

National Assembly. (2015). Civil Code 2015, Law No. 91/2015/QH13, promulgated on 24 November 2015.

National Assembly. (2016). Law on Children 2016, Law No. 102/2016/QH13, promulgated on 5 April 2016.

National Assembly. (2018). Law on Cybersecurity 2018, Law No. 24/2018/QH14, promulgated on 12 June 2018.

Regulation (EU) 2016/679 of the European Parliament and of the Council. (2016). Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Official Journal of the European Union, L 119, 1–88.

Solove, D. J. (2008). Understanding privacy. Harvard University Press.

Solove, D. J., & Hartzog, W. (2022). Breached! Why data security law fails and how to improve it. Oxford University Press.

Van der Sloot, B. (2023). The rights to privacy and data protection and facial recognition technology. In B. Van der Sloot & F. Zuiderveen Borgesius (Eds.), Research handbook on privacy and data protection law (pp. 210–235). Edward Elgar Publishing.

Westin, A. F. (1967). Privacy and freedom. Atheneum.

CHAPTER 3
LEGALISING THE SCREEN: A COMPARATIVE STUDY OF CHILDREN'S SCREEN TIME REGULATION WITH PARTICULAR REFERENCE TO INDIA'S DEVELOPING DIGITAL PROTECTION FRAMEWORK

Prerna ARORA[1]
Sadhna JAIN[2]

[1]Doctorate Scholar, Department of Human Development and Childhood Studies, Lady Irwin College, University of Delhi, New Delhi, India
[2]Professor, Department of Human Development and Family Empowerment, Aditi Mahavidyalaya, University of Delhi, New Delhi, India

INTRODUCTION

A generational shift is taking place in homes, schools, and public areas. Children are growing up with screens as continuous companions. Together, these commonplace behaviours giving children tablets, giving teenagers smartphones, and using algorithms to filter what young people see mark a shift in civilisation. The ramifications go beyond practicality or amusement; they influence the development of friendships, the exploration of identities, and the processing of emotions. This engagement's scope is astounding. Children between the ages of 8 and 12 spend about five hours a day on screen-based entertainment, excluding schoolwork, spend more than seven hours on average (Common Sense Media, 2021).

Excessive screen time has been repeatedly associated with negative developmental outcomes, including as disturbed sleep, decreased physical activity, cognitive problems, and difficulties with emotional and social functioning (Kar *et al*., 2025). Higher screen usage was found to be significantly correlated with emotional symptoms, conduct issues, and depressive tendencies in a cross-sectional study of 670 children aged 6 to14 (Mulla *et al*., 2024). Nearer to home, a survey of 3,624 parents in five northern Indian states found that more than 60% of children between the ages of two and five use screens for two to four hours every day, which is more than what is advised internationally (Bhutani *et al*., 2025).

India's judicial system is still disjointed in spite of these conclusions. Although the DPDP Rules 2025 and the Digital Personal Data Protection Act 2023, which classify children as a sensitive category of data subjects, are significant steps, they lack more comprehensive measures like age-appropriate design codes, school-level device policies, or a specific child digital safety statute (DPO India, 2025; TechPolicy.Press, 2025).

1. THE PROBLEM: SCREEN TIME, CHILD DEVELOPMENT, AND THE REGULATORY VACUUM

Childhood has changed with every significant communication revolution. The internet changed what every child could access, television changed what they could see, and the printing press increased what children could read. On the other hand, the smartphone is a more profound disruption.

It has altered not only what children eat but also how they perceive everyday life because it is small, customised, and constantly connected. In contrast to the television, which can be turned off in the living room, many children grab their smartphones first thing in the morning and last thing at night. Beyond conduct, one must consider biology and development to understand why this is important. A crucial developmental window is occupied by children between the ages of six and fourteen. The prefrontal cortex, which is in charge of long-term cognition, emotional regulation, and impulse control, is still developing.

Attention, empathy, and social cognition neural pathways are being actively moulded and trimmed. The digital environment is crucial in this situation. However, from a neurobiological perspective, the unlimited scroll, quick pleasure, algorithmically selected feeds, and dopamine triggers of notifications that screens offer are nearly the worst conditions for a developing brain. These worries are supported by empirical data. According to a systematic evaluation of eleven randomised controlled trials, interventions that reduced children's screen time enhanced sleep duration by eleven minutes each night and reduced daily exposure by roughly thirty-three minutes, with earlier bedtimes as an additional advantage (Martin *et al*., 2021). Even though they are little, these benefits add up over time since sleep is necessary for hormone balance, memory consolidation, and emotional equilibrium. Small but statistically significant effects from screen-limiting interventions were verified by a meta-analysis of 204 trials, especially those that used structured behavioural strategies including goal-setting and self-monitoring (Jones *et al*., 2021). Another meta-analysis of 41 trials with over 14,000 participants for preschool-aged children showed that early treatments resulted in significant decreases in screen time, highlighting how early childhood is amenable to organised constraints (Wu *et al*., 2025).

The negative effects of excessive screen time go beyond sleep. Higher screen time was consistently associated with decreased physical activity, lower sleep quality, attention problems, and difficulties with emotional and social functioning, according to a study of 46 studies published between 2014 and 2024 (Kar *et al*., 2025).

Screen usage was found to be significantly correlated with emotional symptoms, conduct issues, hyperactivity, and depressed tendencies in a cross-sectional study of 670 children in two Gulf nations. These mental health effects are equally worrying (Mulla *et al*., 2024). Citing hazards to children's physical, mental, and social development, the World Health Organization has officially recommended restricting screen time for children under five (WHO, 2019). Children under five in India, excessive screen use is common and linked to poor developmental outcomes (Khobragade *et al*., 2025).

In 2024, 3,624 parents of children ages two to five in Delhi, Haryana, Uttarakhand, Rajasthan, and Madhya Pradesh participated in a large cross-sectional study. More than 60% of parents said their children used screens for two to four hours per day, which is far more than what is recommended by international standards. However, parents found it difficult to set boundaries, indicating a disconnect between protective behaviour and awareness (Bhutani *et al*., 2025). Interestingly, over one-third of parents never changed their privacy or usage settings not because they were careless, but rather because they were overpowered by platforms that were purposefully made to thwart parental intervention. This aspect of design is very important. Children use platforms that are designed to maximise engagement rather than being neutral technologies. Infinite scroll, autoplay, push notifications, algorithmic recommendations, and social validation metrics are examples of intentional processes of persuasive design, or manipulation, intended to maximise attention and habitual use. Children whose neural defences against them are still developing are subjected to these treatments. This environment's permanence is indicative of a regulatory void.

Conventional child protection law targeted concrete and attributable harms and was based on physical areas, such as homes, workplaces, and schools. In contrast, the digital environment is platform-mediated, algorithmically controlled, borderless, and driven by commercial incentives. Applying frameworks made for the real world to digital ills is similar to using traffic regulations to regulate air quality; the gaps are significant and the fit is not ideal. It is important to comprehend the current wave of digital governance laws in light of this.

Governments are responding to growing facts and the realisation that markets by themselves will not put children's welfare ahead of the profitability of attention, not out of panic.

2. GLOBAL LEGISLATIVE LANDSCAPE: HOW COUNTRIES ARE RESPONDING

A striking convergence of various legal systems, cultures, and political traditions has occurred in a matter of years. Countries that frequently disagree on technology regulation have come to a startling agreement: children need legally binding safeguards in the digital sphere. The tendency is clear: the screen is now a realm that the law aims to regulate, even though approaches vary in scope, mechanism, and ambition.

France: From Classroom Ban to Comprehensive Legislative Regulation

In Europe, France has led the way in legislative action. Beginning with Law No. 2018-698, people up to the age of fifteen were prohibited from using smartphones or other electronic devices in nurseries, primary schools, and middle schools (Library of Congress, 2018). With a few exceptions for educational purposes and people with impairments, this expanded the previous limitations to include the whole school day. Restoring an atmosphere that encourages focus and attention was the obvious justification. The scope was broadened by later actions.

Weak age verification mechanisms have made it difficult to execute France's 2023 law requiring parental approval for minors under the age of fifteen to create social media accounts (Reuters, 2025). In late 2025, President Emmanuel Macron revealed plans to completely prohibit children under the age of fifteen from using social media, citing Australia's legislation as a precedent. In France 2024, the stop numüge project tested full-day smartphone handovers in schools (Reuters, 2025). The course of France serves as an example of how gradual regulation can change social norms and pave the way for more significant reforms.

Australia: The World's Most Ambitious Minimum Age Law

The most comprehensive action in the world is Australia's Online Safety Amendment (social media Minimum Age) Act 2024. Children under the age of sixteen are not allowed to have accounts on popular websites like Facebook, Instagram, TikTok, and YouTube as of December 2025 (Online Safety Amendment Act, 2024; eSafety Commissioner, 2025).

Among the distinguishing characteristics are:

- Platform accountability: platforms, not families, are responsible for compliance.
- Categorical restriction: the prohibition cannot be overridden by parental agreement.
- Technology neutrality: whereas platforms are free to select the mechanisms, they must employ layered age verification techniques.
- Privacy protections: information gathered for verification must be deleted after usage.

UNICEF Australia warned that prohibitions by themselves would force children into less controlled areas, highlighting the necessity of additional safety precautions (UNICEF Australia, 2024).

The United Kingdom: Safety by Design

The sophisticated architecture of the UK's Online Safety Act 2023 is noteworthy. Instead of concentrating only on access, it enforces a safety by design obligation: platforms that children are likely to use must evaluate risks, put mitigations in place, and answer to Ofcom (Online Safety Act, 2023). Important clauses consist of Age verification is required in order to prevent dangerous content including sexual content, eating disorder promotion, and self-harm (Ofcom, 2025). Every time a service is redesigned, there are ongoing risk evaluations. According to DLA Piper (2026), the Children's Wellbeing and Schools Act 2026 permits the digital age of consent to be adjusted between thirteen and sixteen. By incorporating accountability into platform design, this method transfers accountability from families to corporations.

Singapore: Regulating the Pre-School Environment

The youngest children are the focus of Singapore's Grow Well SG campaign. According to regulations, infants under the age of eighteen months are not allowed to use screens at all, and children up to six years old are only allowed to use them for educational purposes (Singapore Ministry of Social and Family Development, 2024). Early childhood provider's licenses are used to enforce compliance. This paradigm emphasises the significance of institutional regulation, acknowledging that when children spend a large amount of time in structured care settings, parental control is insufficient on its own.

The United States: State-Level Innovation Amid Federal Paralysis

The terrain of the United States is fragmented. State-level innovation has progressed while federal initiatives like the Kids Online Safety Act (KOSA) have languished. The SAFE for Kids Act (2023) in New York forbids overnight push alerts and customised algorithmic feeds for minors without parental permission (Children and Screens, 2026). Other states have passed age verification laws for sexual content, but the First Amendment challenges these laws (Kishk, 2024). Two lessons can be learned from the American experience: constitutional safeguards restrict explicit prohibitions, encouraging lawmakers to adopt design-based solutions, and partial regulation runs the danger of developing loopholes.

The European Union: Supranational Governance and the Digital Services Act

The most extensive supranational framework is the EU's Digital Services Act (DSA), which went into full effect in 2024. It imposes additional requirements on Very Large Online Platforms (VLOPs), such as risk assessments, access to researcher data, prohibitions on targeted advertising to minors, and defaulting to age-appropriate privacy settings (European Commission, 2024). Its enforcement capacity is demonstrated by the procedures against TikTok and Meta (Children and Screens, 2026).

The DSA, which is experimenting with multi-level governance that is unmatched elsewhere, exemplifies Europe's ideology of platform accountability and transparency.

3. INDIA'S LEGAL FRAMEWORK: ACHIEVEMENTS, ARCHITECTURE, AND ABSENCES

In terms of global children's digital governance, India holds a unique position. It combines a strong constitutional heritage of fundamental rights with quick smartphone adoption. The recognition of privacy as a basic right following the historic K.S. Puttaswamy v. Union of India (2017) ruling has increased the need of child-centred digital security. However, India lacks a cohesive governance structure that unifies digital design standards, data regulation, and child protection into a single architecture despite these underpinnings.

Foundational Layers: IT Act 2000 and IT Rules 2021

The foundation of India's digital regulations is still the Information Technology Act, 2000. Provisions like Section 67B, which criminalises child sexual abuse material (CSAM), and the IT Rules 2021, which require intermediaries to censor harmful information and facilitate grievance redressal, were not created with children in mind. A proactive step toward enforcement was taken in 2024 with the creation of the SAHYOG site, a centralised mechanism for reporting CSAM and issuing removal orders. However, rather than being a part of a comprehensive framework for child digital safety, these solutions continue to be reactive and dispersed.

The Digital Personal Data Protection Act 2023 and Rules 2025

India's most revolutionary move in digital governance is the DPDP Act 2023. It requires verifiable parental approval before platforms can process children's personal data, and it defines a child as anyone under the age of eighteen, which is a broader threshold than many international frameworks (KSANDK, 2025). Through connection with Digi Locker, the DPDP Rules 2025 operationalise this by outlawing targeted advertising, behavioural tracking, and profiling of children (DPDP Rules, 2025).

Although this framework is important, its use is constrained. It controls data processing, not the digital environment as a whole. Screen time, persuasive design elements, and algorithmic systems that influence children's experiences are not covered. In this regard, the DPDP Act is an essential starting point but not an adequate remedy.

Constitutional Dimension

Strong normative backing for child digital safety is provided by India's constitutional framework. The State is clearly obligated under Article 21's recognition of privacy, Article 21A's promise of free education, and Article 39(f)'s duty to safeguard children from exploitation. Protection and respect for children's growing autonomy must be balanced in any future child-centred digital governance framework; this is a problem that is simpler to describe than to enact.

4. CRITICAL ANALYSIS: GAPS, CHALLENGES, AND THE LIMITS OF LAW

After examining both India's internal legal framework and the global legislative scene, it is imperative to address the structural limitations of regulation. Even while the screen time rule is well-designed, there are issues with it that are not specific to India but are quite noticeable there. These limitations must be addressed in any meaningful policy study.

The Enforcement Gap

Without enforcement, legislation is merely a goal with no real consequences. This is exemplified by India's experience with the DPDP Act, which was passed in August 2023 but its implementing rules were not announced until November 2025, a delay of more than two years during which the statute was essentially inert (TechPolicy.Press, 2025). As of right now, substantive duties won't be enforced until May 2027. According to this schedule, children between the ages of nine and fourteen most actively negotiating digital risks won't receive significant protection under India's most progressive statute until they are getting close to adulthood. Delays are not the only issues with enforcement.

They are institutional, technological, and jurisdictional. Since the headquarters of major sites like Instagram, YouTube, Snapchat, and TikTok are located outside of India, compliance depends on difficult negotiations and real risks of market exclusion. The process of age verification itself presents significant challenges because children can falsify their age, use family members' accounts, get around limits by using VPNs, or switch to other platforms when they are barred (Kishk, 2024). The DPDP Rules' reliance on DigiLocker is predicated on the assumption that digital infrastructure and literacy are unevenly distributed throughout India, with strong levels in urban families and much lower levels in rural and semi-urban areas.

The Digital Divide: When Protection Becomes Exclusion

The possibility that one child's protection will result in another's exclusion is a structurally important challenge. The digital divide in India is glaring. In comparison to 47.29% in urban regions, just 18.47% of rural schools have internet connectivity (Sadashiv, 2024). Smartphones are not diversions for many children in semi-urban and rural areas; rather, they are their main source of social interaction, education, and knowledge (Mapsofindia, 2021). This gap is exacerbated by gender inequality and caste. Men are over twice as likely as women to use the internet, and Scheduled Tribe households report much lower internet access than dominant caste homes, especially in metropolitan settings (IDR Online, 2026; NIIT Foundation, 2024). Children who rely on digital tools for learning run the risk of being penalised by a universal rule that caps screen time or restricts platform access.

The Parental Consent Conundrum

Serious issues are raised by the DPDP Act's emphasis on verifiable parental consent as the cornerstone of child protection. Digi Locker verification assumes time, knowledge, and documentation, all of which are lacking in many households (TechPolicy). Press, 2025). It is unrealistic for children who require access to crisis support, healthcare information, or educational platforms to wait for bureaucratic consent procedures. The model is further complicated by adolescent autonomy.

Particularly in hazardous homes, a seventeen-year-old seeking mental health care, LGBTQ+ resources, or legal aid may have the maturity and need to seek services without parental involvement. The discrepancy between the lived reality of children's digital existence and the legal model of parental consent is a design issue rather than a small implementation error. The digital age of consent is set between thirteen and sixteen in other jurisdictions, including the UK, which permits flexibility. Such gradations are not allowed under India's uniform age-eighteen barrier.

Privacy, Surveillance, and the Paradox of Age Verification

Despite their good intentions, age verification systems pose a threat to civil liberties and privacy. Platforms that must validate age using government IDs, identity documents, or biometric estimation inevitably gather more personal information. This creates a paradox: in order to safeguard children's data, authorities mandate that platforms gather more of it. Fairness issues regarding which children are more likely to be mistaken or excluded have been raised by research showing racial and gender bias in algorithmic age estimate (Livingstone *et al*., 2024). If stringent minimisation and destruction regulations are not followed, the gathering of identity documents for age assurance raises the possibility of data breaches and surveillance, which disproportionately affect vulnerable users (Jarvie *et al*., 2024). An uncommon safeguard is Australia's mandate that verification data be deleted after use; most frameworks leave privacy protections up to platform discretion, which a reliance history indicates is misguided.

The Problem with Time-Based Restrictions

Finally, when it comes to time-based limitations, prudence is necessary. There is surprisingly little evidence that modest time constraints, such as one hour daily or two hours on weekends, result in appreciable gains in wellbeing. Once demographic factors were taken into account, population-based research of almost 20,000 children between the ages of two and five revealed no discernible benefit for those who adhered to suggested screen time limits over those who did not (Przybylski & Weinstein, 2019).

Small and non-linear associations were found. It's important to consider not just how much time children spend on screens, but also what they do, with whom, and in what situations. A regulation that just considers duration runs the danger of measuring the incorrect variable. Design architecture, social context, and content quality must all be addressed concurrently for effective governance.

5. THE WAY FORWARD: POLICY RECOMMENDATIONS FOR INDIA

India has the institutional ability in organisations like the NCPCR, MeitY, and the planned Data Protection Board, as well as the constitutional underpinnings and legislative aspirations through the DPDP framework. A cogent architecture, a child-centred, rights-consistent digital governance framework that incorporates international best practices while staying rooted in India's unique realities is what is lacking. The suggestions that follow are aimed at achieving that objective.

A Dedicated Children's Digital Safety Act

India needs a Children's Digital Safety Act, a stand-alone law that unifies the protections included in the DPDP Act, POCSO, and IT Act. Minimum age restrictions for social media access, design guidelines for platforms that interact with children, developmentally appropriate content standards, and age verification frameworks with required data minimisation should all be incorporated into such laws. Foreign platforms operating in India must be covered by enforcement procedures. Every time major design changes are made, platforms should be obliged to perform and disclose children safety risk assessments, taking inspiration from the UK's systems-accountability model. As a statutory co-regulator under this Act, the National Commission for Protection of Child Rights (NCPCR) should have jurisdiction over digital harms and the competence to give platforms legally binding directives.

An Age-Appropriate Design Code

A mandated Age-Appropriate Design Code, based on the UK's 2020 framework, ought to be implemented in India.

In situations where minors are expected to utilise the platform, this would necessitate the implementation of particular design standards. The highest level of privacy settings should be the default; children should not be encouraged to choose privacy-invasive options; commercial child profiling should be prohibited; autoplay should be limited; and design elements that take advantage of psychological weaknesses should not be allowed. Instead of depending on reactive enforcement, such a code would target the architecture of damage itself, integrating prevention into design.

Differentiated Age Thresholds for Parental Consent

Every individual under the age of eighteen is considered a child for data protection reasons under India's Digital Personal Data Protection Act (DPDP) 2023, which takes a moral stance. This indicates the legislature's dedication to providing complete protection for minors and reflects the domestic age of majority (KSANDK, 2025). The threshold fits India's framework with its own legal system and is more expansive than a number of international regimes, such as the Children's Online Privacy Protection Act (COPPA) of the United States, which defines a child as under thirteen. However, practical workability is not necessarily correlated with legal consistency. When it comes to parental consent, treating a seven-year-old and a seventeen-year-old in the same way oversimplifies developmental realities and threatens the theoretical underpinnings of the law. A corrective lens is provided by the United Nations Convention on the Rights of the Child (UNCRC), which India adopted in 1992 (United Nations, 1989). Article 5 acknowledges the child's changing abilities and emphasises that parental responsibilities must change as children grow, moving from direct supervision in the early years to discussion and collaborative decision-making in adolescence (United Nations, 1989). While older adolescents are becoming more capable of exercising judgement, youngsters need more protection because they are less able to understand consequences (United Nations, 1989). The fundamental tenet of the UNCRC is violated by a consent framework that disregards this developmental cycle and treats preteens and near-adults as legally equal. This progressive logic is reflected in global practice (Parkes, 2019).

The default age of digital consent is sixteen, although Member States may reduce it to thirteen under Article 8 of the EU General Data Protection Regulation (GDPR) (European Union, 2016). Thirteen in Spain, Ireland, Denmark, and Sweden; fourteen in Austria and Italy; and sixteen in Germany, the Netherlands, and Hungary are the actual thresholds (European Union, 2016). This variation is realism rather than incoherence; it recognises that developmental capability varies and needs to be adjusted to national social and cultural settings.

India should adopt a three-tiered consent framework based on this comparable basis. In accordance with both GDPR and developmental evidence, complete and verifiable parental authorisation must continue to be required before any platform handles the data of children under the age of thirteen (European Union, 2016). Children between the ages of thirteen and fifteen should be able to independently access specific categories of services, such as educational tools, health and wellbeing platforms, and crisis or mental health support, without parental authorisation. However, commercial social media and engagement-driven consumer applications should still require parental consent.

This is equity rather than permissiveness: an adolescent experiencing identity-related anguish, family violence, or mental health issues shouldn't be prevented from seeking professional assistance just because parental consent is lacking or hazardous (Parkes, 2019). Given their close closeness to legal majority and growing competence, adolescents between the ages of sixteen and seventeen should be granted significantly more autonomy (United Nations, 1989; Parkes, 2019). Although it should not be a strict requirement for every data processing, parental consent may nevertheless be given as a safeguard. The protection of children is not compromised by this distinction. Conversely, it makes it stronger by bringing India's framework into line with international norms, developmental science, and constitutional principles.

Platform Accountability and Mandatory Reporting

The current system in India is overly dependent on enforcement through complaints. Large-scale platforms must to be obliged to release yearly transparency reports that are broken down by user age and include information on the number of users under the age of eighteen.

The types of harms that have been reported, the design elements intended for younger users, and the actions made to reduce risks. In order to create overlapping accountability duties and lower the danger of regulatory capture, these reports should be sent to both the Data Protection Board and the National Commission for Protection of Child Rights (NCPCR).

Digital Equity as a Non-Negotiable Design Constraint

Child digital governance must be designed for the full spectrum of Indian childhood not only urban, middle-class children with digitally literate parents, but also semi-urban and rural children who share devices, first-generation internet users whose parents cannot navigate Digi Locker, and adolescents for whom the internet is the only window to the wider world. Regulation that excludes these children is not protection; it is selective protection, which is itself a form of inequality. Practical measures include: alternative consent verification pathways that do not rely solely on Digi Locker or identity documents; school-based digital literacy programmes for children and parents; and exemptions from age-verification requirements for educational, health, and welfare services, ensuring that children most in need of support are not blocked by poorly calibrated legal requirements.

Anchoring the Framework in the UNCRC

In 1992, India ratified the United Nations Convention on the Rights of the Child (UNCRC). Article 17 requires nations to safeguard minors from dangerous content while guaranteeing their right to appropriate information. The dual mandate of protection and access ought to be the fundamental tenet that governs India's digital governance for children. Neither a framework that merely permits nor one that merely restricts is UNCRC-compliant. A digital space where all children can engage in meaningful, safe, and autonomous activities must be the aim.

CONCLUSION

In the twenty first century the way power manifests itself is novel. These days, technology companies' product roadmap meetings, engineers' algorithmic design judgements, and boardrooms where engagement metrics take precedence over child welfare are where the most significant decisions influencing children's developmental settings are made, not in factories or classrooms. The legislative response to this fact around the world is promising. The most ambitious minimum-age social media law in history was passed in Australia. France has transitioned from classroom prohibitions to all-encompassing regulations that cover platforms and schools.

The UK is a leader in systems-level accountability. Singapore has protected its youngest children in institutional environments. Through the Digital Services Act, the European Union has used its regulatory power to force the biggest platforms to comply. There is a growing consensus among these jurisdictions that the digital world is not neutral, children are not sufficiently safeguarded by current legislation, and markets will not provide the necessary safeguards.

India is at a critical point right now. The biggest development since the IT Act is the DPDP Act 2023 and Rules 2025, which constitute a considerable advancement. There are constitutional underpinnings for a rights-based system. The institutional actors are real and have the potential to gain power. All that is left is the determination to construct the architecture that these foundations require: a specific Children's Digital Safety Act, an Age-Appropriate Design Code, distinct consent thresholds, required platform transparency, and, most importantly, a framework created for the varied realities of Indian childhood.

The years between six and fourteen are among the most important for human development, according to developmental research. It is not a technical issue, but rather the legislative framework that controls what children experience during those years whose attention is captivated, whose data is harvested, whose emotions are manipulated. It comes down to the kind of society India wants to have and what it thinks its kids should be entitled to. The screen is already governed by law. The only unanswered concern is whether India's legislation would be sufficiently ambitious to address the magnitude of the issues involved.

REFERENCES

Bhutani, P., Arora, K., Singh, N., Garg, A., Agarwal, A., & Bhutani, J. (2025). Analysis of parental beliefs and practices leading to excessive screen time in early childhood. BMJ Paediatrics Open, 9(1). https://doi.org/10.1136/bmjpo-2024

Children and Screens. (2026, January). Policy update: January 2026. https://www.childrenandscreens.org/newsroom/news/policy-update-january-2026/

Digital Personal Data Protection Act, No. 22 of 2023 (India). (2023). Ministry of Electronics and Information Technology. https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

Digital Personal Data Protection Rules, 2025. (2025). Ministry of Electronics and Information Technology, Government of India. https://www.meity.gov.in/

DLA Piper. (2026, April). Online Safety Act: New steps towards restricting children's access online. https://www.dlapiper.com/

eSafety Commissioner, Australia. (2025, September). Regulatory guidance on social media minimum age. Australian Government. https://www.esafety.gov.au/

European Commission. (2024). Digital Services Act: Commission opens proceedings against TikTok and Meta. https://ec.europa.eu/

European Union. (2016). General Data Protection Regulation, Article 8 — Conditions applicable to child's consent in relation to information society services. Regulation (EU) 2016/679 of the European Parliament and of the Council. https://gdpr-info.eu/art-8-gdpr/

France24. (2024, September 4). Digital pause: France pilots school mobile phone ban. https://www.france24.com/en/live-news/20240904-digital-pause-france-pilots-school-mobile-phone-ban

IDR Online. (2026, January). The digital wall: How caste shapes access to technology in India. https://idronline.org/

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India). (2021). Government of India.

Information Technology Act, No. 21 of 2000 (India). (2000). Government of India.

Jarvie, C., Livingstone, S., & Stoilova, M. (2024). Online age verification: Government legislation, supplier responsibilization, and public perceptions. Children, 11(4). https://doi.org/10.3390/children11040452

Jones, A., Armstrong, B., Weaver, R. G., Parker, H., von Klinggraeff, L., & Beets, M. W. (2021). Identifying effective intervention strategies to reduce children's screen time: A systematic review and meta-analysis. International Journal of Behavioral Nutrition and Physical Activity, 18(1), Article 126. https://doi.org/10.1186/s12966-021-01189-6

Kar, S. S., Dube, R., Goud, B. K. M., Gibrata, Q. S., El-Balbissi, A. A., Al Salim, T. A., & Fatayerji, R. N. M. A. K. (2025). Impact of screen time on development of children. Children, 12(10), 1297. https://doi.org/10.3390/children12101297

Khobragade, R., Dhar, M., Singh, T., & Bajaj, N. (2025). Screen time among under-five children in India: A systematic review and meta-analysis. Cureus, 17(6). https://doi.org/10.7759/cureus.376322

Kishk, Y. (2024). State-based online restrictions: Age-verification and the VPN obstacle in the law. International Journal of Law, Ethics, and Technology, 3(1), 45–67.

KSANDK Law. (2025). Children's data under the DPDP Act, 2023 and DPDP Rules, 2025. https://ksandk.com/

Library of Congress. (2018, October 30). France: Government adopts law banning cell phone use at school. https://www.loc.gov/item/global-legal-monitor/2018-10-30/france-government-adopts-law-banning-cell-phone-use-at-school/

Livingstone, S., Stoilova, M., & Nandagiri, R. (2024). Children's rights and online age assurance systems. The International Journal of Children's Rights, 32(2), 418–445. https://doi.org/10.1163/15718182-32020004

Martin, K. B., Bednarz, J. M., & Aromataris, E. C. (2021). Interventions to control children's screen use and their effect on sleep: A systematic review and meta-analysis. Journal of Sleep Research, 30(3), e13130. https://doi.org/10.1111/jsr.13130

Mulla, W., Ahmed, W., Radhi, M., Alaali, H., Alwazeer, G., Yusuf, F., Alsuhim, G., Al Suhaym, A., Alahmari, W., Abdulla, M., & Yusuf, E. (2024). Exploring screen time and its effects on children's mental health: A cross-sectional study. Cureus, 16(10), e71215. https://doi.org/10.7759/cureus.71215

Observer Research Foundation. (2025). DPDP Rules and the future of child data safety. https://www.orfonline.org/

Ofcom. (2025). Children's safety codes and guidance. https://www.ofcom.org.uk/

Online Safety Act 2023, c. 50 (United Kingdom). (2023). Government of the United Kingdom. https://www.legislation.gov.uk/ukpga/2023/50 (legislation.gov.uk in Bing)

Online Safety Amendment (Social Media Minimum Age) Act 2024 (Cth) (Australia). (2024). Federal Register of Legislation. https://www.legislation.gov.au/C2024A00127/asmade/text (legislation.gov.au in Bing)

Parkes, A. (2019). The principle of evolving capacities under the UN Convention on the Rights of the Child. The International Journal of Children's Rights, 27(2), 306–337. https://doi.org/10.1163/15718182-02702003

Protection of Children from Sexual Offences Act, No. 32 of 2012 (India). (2012). Government of India.

Przybylski, A. K., & Weinstein, N. (2019). Digital screen time limits and young children's psychological well-being: Evidence from a population-based study. Child Development, 90(1), e56–e65. https://doi.org/10.1111/cdev.13007

Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1 (India). (2017). Supreme Court of India.

Reuters. (2025, December 31). Macron wants to ban under-15s from social media from September 2026. https://www.reuters.com/

Sadashiv K, S. (2024, November 29). Rural schools lag 29% behind urban in internet access: Education Ministry data. Medianama. https://www.medianama.com/2024/11/223-29-per-cent-disparity-rural-urban-schools-internet-access-education-ministry-data/

TechPolicy.Press. (2025, July 22). Parental consent is a conundrum for online child safety. https://www.techpolicy.press/

UNICEF Australia. (2024). Social media ban explainer. https://www.unicef.org.au/

United Nations. (1989). Convention on the Rights of the Child, Articles 5 and 12. UN General Assembly Resolution 44/25. https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

United Nations. (1989). Convention on the Rights of the Child. UN General Assembly Resolution 44/25. https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

World Health Organization. (2019). Guidelines on physical activity, sedentary behaviour and sleep for children under 5 years of age. https://iris.who.int/handle/10665/311664

Wu, Y., Xi, X., Zhang, C., Jiang, J., & Ye, S. (2025). Effect of intervention on screen time in preschoolers: A systematic review and meta-analysis of randomised controlled trials. *BMC Public Health, 25*, 2724. https://doi.org/10.1186/s12889-025-23700-5

978-625-91851-6-3