INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

TECHNOLOGICAL ADVANCEMENTS AND THE REGULATION OF MOBILE APPLICATIONS: CHALLENGES, GAPS, AND THE PATH FORWARD

AUTHORED BY - ISHWAR CHANDRA ROY
Ph.D. Research Scholar, Chanakya National Law University, Patna

ABSTRACT

The proliferation of mobile applications, accelerated by the integration of Artificial Intelligence (AI), Machine Learning (ML), and Blockchain technology, has fundamentally reshaped the digital economy. While these technologies expand functionality and user engagement, they simultaneously produce regulatory challenges that existing legal frameworks are ill-equipped to address. This article examines three interconnected dimensions of this regulatory deficit: (i) the opacity and ethical hazards of AI- and ML-driven applications; (ii) the jurisdictional, contractual, and anonymity problems generated by Blockchain-based mobile platforms; and (iii) the structural causes of regulatory lag, including inadequate technical literacy among policymakers and the absence of harmonised global standards. Drawing on existing regulatory frameworks—including the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and India's Digital Personal Data Protection Act, 2023—the article identifies critical gaps and advances a set of reform proposals centred on adaptive governance, interdisciplinary collaboration, mandatory algorithmic transparency, and global standardisation. The article concludes that effective regulation of mobile applications requires a shift from reactive rule-making to proactive, ethics-grounded, and technically informed governance.

Keywords: Mobile Applications, Artificial Intelligence, Machine Learning, Blockchain, Data Privacy, GDPR, DPDP Act, Regulatory Lag, Algorithmic Accountability, Global Standardisation.

ISSN: 2582-6433

I. INTRODUCTION

The past two decades have witnessed an exponential expansion in the global mobile application market. Once confined to basic utilities, mobile applications today constitute sophisticated, autonomous systems that learn from user behaviour, conduct financial transactions, and mediate access to essential services in healthcare, finance, education, and commerce. This transformation has been driven, in large part, by the embedding of Artificial Intelligence (AI), Machine Learning (ML), and Blockchain technology into mobile platforms.[1]

While these technologies enhance functionality and personalisation, they simultaneously generate novel legal and ethical challenges. AI-driven applications process vast quantities of sensitive personal data through opaque algorithmic processes, raising profound concerns about transparency, discrimination, and informed consent. Blockchain-based applications, by virtue of their decentralised architecture, defy the territorial assumptions on which most regulatory regimes are constructed. [2] Together, these developments have exposed fundamental inadequacies in existing regulatory frameworks—frameworks that were largely designed for a less dynamic, more centralised digital environment.

The challenge for regulators is not merely technical but structural. Regulatory institutions typically operate through deliberate, multi-stage processes—consultation, drafting, legislative debate, and enforcement—that cannot match the pace at which mobile technologies evolve. The result is a persistent regulatory lag, compounded by insufficient technical expertise within legislative and administrative bodies and the absence of a coherent international framework capable of governing applications that operate seamlessly across jurisdictions.

This article proceeds in six parts. Part II analyses the regulatory implications of AI and ML in mobile applications, focusing on algorithmic opacity, data privacy, and the manipulation of user autonomy. Part III examines the challenges posed by Blockchain technology, including jurisdictional ambiguity, the legal enforceability of smart contracts, and the facilitation of illicit activity through pseudonymous transactions. Part IV assesses the structural causes of regulatory failure—regulatory lag and the deficit of technical expertise. Part V considers the

[1] O. Akpobome, The Impact of Emerging Technologies on Legal Frameworks: A Model for Adaptive Regulation, 5 Int'l J. Res. Pub. & Rev. 5046, 5046–5060 (2024).
[2] O. Kuznetsov et al., On the Integration of Artificial Intelligence and Blockchain Technology: A Perspective About Security, 12 IEEE Access 3881, 3881–3897 (2024).

ISSN: 2582-6433

challenge of global harmonisation. Part VI proposes a comprehensive set of reforms. The article concludes with reflections on the kind of regulatory imagination that the current moment demands.[3]

II. ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN MOBILE APPLICATIONS: REGULATORY CONSIDERATIONS

A. Algorithmic Opacity and Accountability

Perhaps the most pressing regulatory concern arising from the integration of AI and ML into mobile applications is the problem of algorithmic opacity—commonly termed the 'black box' problem. Many contemporary ML systems, particularly those employing deep learning architectures, produce outputs through processes that are opaque even to their designers. The statistical complexity of multi-layered neural networks makes it exceedingly difficult to trace a given output to its causal antecedents.[4]

This opacity carries significant legal and ethical implications in high-stakes domains such as credit assessment, healthcare, and employment. Consider a mobile lending application that evaluates creditworthiness using data points including browser history, geolocation, and social media behaviour. A user denied credit may have no meaningful way of understanding or challenging the decision. More troublingly, the algorithm may be utilising proxies that correlate with protected characteristics—race, gender, or socioeconomic status—thereby producing discriminatory outcomes without any deliberate discriminatory intent.[5]

Existing legal regimes have not adequately addressed this problem. Although the GDPR introduces a limited 'right to explanation' in the context of automated decision-making, the practical scope of this right remains contested, and enforcement has been inconsistent.[6] The absence of robust requirements compelling algorithmic transparency has allowed firms to resist disclosure by invoking trade secret protections. Without clear regulatory mandates, the deployment of black-box AI systems in consumer-facing mobile applications will continue to erode user trust and create conditions for unchecked discrimination.

[3] K.A. Yaeger et al., United States Regulatory Approval of Medical Devices and Software Applications Enhanced by Artificial Intelligence, 8 Health Pol'y & Tech. 192, 192–197 (2019).
[4] Simon Chesterman, Through a Glass, Darkly: Artificial Intelligence and the Problem of Opacity, 69 Am. J. Comp. L. 271, 271–294 (2021).
[5] Anya E. Prince & Daniel Schwarcz, Proxy Discrimination in the Age of Artificial Intelligence and Big Data, 105 Iowa L. Rev. 1257 (2019).
[6] Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius, The European Union General Data Protection Regulation: What It Is and What It Means, 28 Info. & Commc'ns Tech. L. 65, 65–98 (2019).

ISSN: 2582-6433

B. Data Privacy and the Limits of Consent

A related concern involves the manner in which AI- and ML-driven mobile applications collect and process personal data. The performance of these systems depends on continuous access to large, varied datasets—often including sensitive behavioural, locational, and biometric information. While this data enables personalisation and predictive functionality, it also raises acute questions about privacy, consent, and purpose limitation.[7]

Mobile applications commonly obtain user consent through lengthy, opaque terms of service presented at the point of installation. These instruments are rarely read and are frequently drafted in technical or legalistic language that renders meaningful comprehension impractical. Users accordingly consent—often broadly and irrevocably—to data collection practices they do not fully understand.[8]

Even where initial consent is obtained, the dynamic character of AI-driven data processing challenges the coherence of consent as a regulatory mechanism. AI models do not merely process data as initially collected; they continuously generate new inferences from evolving data streams, raising the question of whether the original consent extends to these subsequent uses.[9] The widespread embedding of third-party Software Development Kits (SDKs) in mobile applications compounds this problem, creating complex data-sharing arrangements that are opaque to both users and regulators.[10]

The inadequacy of notice-and-consent frameworks in the context of AI-driven data processing has prompted calls for a more structural approach to privacy regulation—one that emphasises privacy-by-design, purpose limitation, and data minimisation as affirmative technical requirements rather than aspirational standards.

C. Personalisation, Manipulation, and User Autonomy

Personalisation, a defining feature of AI-powered mobile applications, occupies an ambiguous normative position. While curated experiences enhance user utility, the same algorithmic mechanisms can be deployed to exploit cognitive biases and override rational agency. Engagement-maximising platforms—social media, e-commerce, and gaming

[7] European Parliament and Council Regulation 2016/679, General Data Protection Regulation art. 5(1)(b), 2016 O.J. (L 119) 1 [hereinafter GDPR].
[8] Adeniyi A.O. et al., Ethical Considerations in Healthcare IT: A Review of Data Privacy and Patient Consent Issues, 21 World J. Advanced Res. & Revs. 1660, 1661 (2024).
[9] F.H. Cate & V. Mayer-Schönberger, Notice and Consent in a World of Big Data, 3 Int'l Data Privacy L. 67, 68–72 (2013).
[10] M.R. Asghar et al., A Review of Privacy and Consent Management in Healthcare: A Focus on Emerging Data Sources, in 2017 IEEE 13th Int'l Conf. on e-Science 518, 519–20 (2017).

ISSN: 2582-6433

applications—routinely exploit predictive models to identify users' moments of vulnerability and target them with inducements calibrated to maximise conversion rates.[11]

The legal literature has begun to grapple with the distinction between legitimate personalisation and algorithmically mediated manipulation. Existing consumer protection legislation, premised on models of rational choice and informed consent, is ill-suited to address behavioural manipulation that operates below the threshold of conscious awareness. The causal relationship between algorithmic design and user harm is difficult to establish, making legal redress problematic.[12]

Particular concern attaches to the vulnerability of specific population groups. Children, elderly users, and persons with limited digital literacy are especially susceptible to algorithmic influence. The absence of heightened regulatory protections for these groups in most existing frameworks reflects a significant normative lacuna that future legislation must address.

III. BLOCKCHAIN TECHNOLOGY IN MOBILE APPLICATIONS: REGULATORY CHALLENGES

A. Decentralisation and Jurisdictional Ambiguity

Blockchain's defining architectural feature—decentralisation—is simultaneously its principal regulatory challenge. Unlike conventional client-server systems in which data and operations are housed within geographically determinate infrastructure, blockchain networks distribute their nodes across multiple jurisdictions without any single point of control. This design principle, while conferring significant security and resilience advantages, renders it effectively impossible to identify a legally responsible entity for a given transaction or operation.[13]

Consider a cryptocurrency wallet application developed by a team in Germany, used by an individual in India, and operating on a blockchain whose nodes are distributed across Canada, Japan, and Brazil. In the event of a dispute—whether involving an unauthorised transaction, a data breach, or a regulatory violation—the identification of the applicable law and the competent forum presents an intractable problem. Conventional territorial jurisdiction, which assigns legal responsibility on the basis of geographic presence, is inadequate to govern

[11] E. Kavoliūnaitė-Ragauskienė, Artificial Intelligence in Manipulation: The Significance and Strategies for Prevention, 17 Baltic J. L. & Pol. 116, 117–21 (2024).
[12] H. Lemsieh & I. Abarar, Artificial Intelligence: A Technological Tool to Manipulate the Psychology and Behavior of Consumers, 5 Int'l J. Accounting, Fin., Auditing, Mgmt. & Econ. 432, 434–36 (2024).
[13] Z. Wenhua et al., Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends, 12 Electronics 546, 546–48 (2023).

ISSN: 2582-6433

entities and transactions that are, by design, geographically indeterminate.[14]

The challenge is compounded by the use of decentralised autonomous organisations (DAOs) and decentralised storage systems such as the InterPlanetary File System (IPFS), which eliminate identifiable intermediaries entirely. In the absence of an entity against which regulatory and enforcement action can be directed, the practical reach of national and regional regulators is severely limited. Despite growing interest at multilateral forums including the G20, no harmonised framework has emerged to address this jurisdictional deficit.

B. Smart Contracts and the Question of Legal Enforceability

Smart contracts—self-executing agreements whose terms are encoded directly into blockchain protocols—represent one of the most transformative and legally vexed features of blockchain-based mobile applications. Used in contexts ranging from subscription management and in-app purchases to decentralised lending and identity verification, smart contracts automate contractual obligations and eliminate the need for intermediaries.[15]

Yet their legal status remains deeply uncertain. Classical contract law requires mutual assent, certainty of terms, and the possibility of judicial interpretation in the event of ambiguity or breach. Smart contracts, encoded in programming language, afford minimal scope for contextual interpretation. A coding error or unforeseen contingency may cause a smart contract to execute in ways that produce plainly unjust results, with no mechanism for appeal or reconsideration.[16]

The immutability of blockchain further exacerbates this problem. Once deployed, a smart contract cannot be modified without consensus across the network—a requirement that may be practically insurmountable. In addition, the anonymity or pseudonymity of contracting parties may make it impossible to serve legal process, even where a competent forum can be identified.[17] While a small number of jurisdictions—Arizona and Tennessee in the United States—have enacted legislation recognising smart contracts as legally enforceable instruments, this remains the exception rather than the rule. No international consensus exists regarding the legal treatment of smart contracts, leaving a significant gap in the governance of blockchain-based mobile transactions.

[14] D. Marbouh et al., A Blockchain-Based Regulatory Framework for mHealth, 7 Data 177, 178–80 (2022).
[15] M. Giancaspro, Is a 'Smart Contract' Really a Smart Idea? Insights from a Legal Perspective, 33 Computer L. & Security Rev. 825, 827–30 (2017).
[16] V. Dwivedi et al., Legally Enforceable Smart-Contract Languages: A Systematic Literature Review, 54 ACM Computing Surveys 1, 3–8 (2021).
[17] N. Kannengiesser et al., Challenges and Common Solutions in Smart Contract Development, 48 IEEE Transactions on Software Eng'g 4291, 4295–98 (2021).

ISSN: 2582-6433

C. Anonymity and the Facilitation of Illicit Activity

A further regulatory challenge arises from the pseudonymity that blockchain technology affords to its users. In blockchain-based mobile applications, users are typically represented by alphanumeric wallet addresses rather than verifiable identities. While this feature protects user privacy and enables censorship-resistant communication, it also creates conditions that are conducive to financial crime, tax evasion, and the distribution of illegal content.[18]

Decentralised exchanges and peer-to-peer payment applications rarely obtain meaningful identity verification from users, and even where Know Your Customer (KYC) and Anti-Money Laundering (AML) procedures are nominally observed, they are frequently superficial or susceptible to circumvention. The anonymity of developers and operators—many blockchain applications are released by pseudonymous collectives—means that users who suffer loss through application defects or fraudulent conduct often have no recourse.

Governmental efforts to impose regulatory requirements on blockchain developers and service providers have met with limited success. The prohibition of a mobile application in one jurisdiction does little to restrict access where applications are hosted on decentralised platforms or distributed through unofficial channels. The absence of effective enforcement mechanisms represents a serious limitation on the regulatory capacity of nation-states in this domain.

IV. REGULATORY LAG AND THE DEFICIT OF TECHNICAL EXPERTISE

A structural cause of the regulatory inadequacies identified in the preceding Parts is the well-documented phenomenon of regulatory lag—the gap between the pace of technological innovation and the capacity of legislative and administrative institutions to respond. Mobile applications are subject to continuous iteration; new AI models and blockchain capabilities are deployed faster than regulatory processes can assimilate and evaluate them. By the time a regulatory instrument is finalised, the technology it was designed to govern may have evolved beyond recognition.[19]

[18] M. Blaszczyk, Blockchain and Private Law (Jan. 2023) (unpublished manuscript), https://ssrn.com/abstract=4319649.

[19] Organisation for Economic Co-operation and Development, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013), https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

ISSN: 2582-6433

This temporal mismatch is exacerbated by a second, related deficit: the shortage of technical expertise within regulatory institutions. Most legislators and regulatory officials lack formal training in computer science, data science, or digital systems engineering. This knowledge gap inhibits the formulation of technically sound and practically feasible regulatory requirements, and renders institutions dependent on industry-supplied information—a dependence that carries obvious risks of regulatory capture.

Some jurisdictions have begun to experiment with adaptive regulatory models designed to address these structural limitations. Regulatory sandboxes—controlled environments in which developers may test novel products under regulatory supervision without automatic legal liability—have been adopted in a number of FinTech contexts and have demonstrated some potential for bridging the gap between innovation and regulation. However, sandbox programmes remain limited in geographic scope and have yet to be systematically extended to AI-driven or blockchain-based mobile applications.[20]

The establishment of technology advisory boards within regulatory bodies—comprising experts in AI, blockchain, cybersecurity, and related fields—represents a second important institutional response. Such bodies can provide technically informed guidance at the policy-drafting stage and assist regulators in anticipating the implications of emerging developments. Their effectiveness depends, however, on sustained funding, genuine institutional independence, and the willingness of policymakers to engage with technical complexity rather than defer to industry framing.

Addressing regulatory lag ultimately requires a systemic reform of the relationship between technical expertise and governance. Academic institutions, civil society organisations, and independent research centres must be actively integrated into policy processes. Ongoing professional education for legislators and regulators—focused specifically on the interface between law and digital technology—is a prerequisite for informed, evidence-based policymaking.

[20] California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100–1798.199 (2018) [hereinafter CCPA].

ISSN: 2582-6433

V. THE CHALLENGE OF GLOBAL STANDARDISATION

The cross-border character of mobile applications makes the absence of a coherent international regulatory framework particularly consequential. Applications are routinely developed in one jurisdiction, hosted in another, and used by hundreds of millions of people across the world. Yet the legal frameworks that govern them remain primarily national or regional in character, producing a fragmented regulatory landscape that creates compliance challenges for developers and leaves users exposed to inconsistent levels of protection.[21]

The divergence among existing regulatory approaches illustrates the scale of the challenge. The European Union's rights-based model—anchored by the GDPR and, increasingly, the proposed Artificial Intelligence Act—emphasises individual rights, transparency, and accountability. The United States, by contrast, relies on a sectoral patchwork of federal and state legislation, prioritising market flexibility and innovation. China's approach is characterised by state control over digital infrastructure, mandatory data localisation, and algorithmic supervision oriented towards national security objectives. India, through the Digital Personal Data Protection Act, 2023, has sought to balance user rights and economic growth in a rapidly expanding digital economy.

This regulatory pluralism creates a range of practical difficulties. Developers seeking to operate globally must simultaneously satisfy conflicting requirements—the GDPR's prohibition on certain international data transfers, China's data localisation mandates, and India's evolving consent requirements are not easily reconciled. Compliance costs fall disproportionately on smaller developers and startups, potentially reinforcing market concentration in favour of large platforms with the resources to navigate complex multi-jurisdictional environments.[22]

The major app distribution platforms—the Apple App Store and Google Play—function as de facto gatekeepers of the mobile application ecosystem, but they operate without systematic regulatory oversight and apply their own content and privacy policies in ways that are neither transparent nor democratically accountable.[23][24] The possibility of sideloading—

[21] Personal Data Protection Bill, 2019, No. 373 of 2019 (India).
[22] Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India).
[23] Apple Inc., App Store Review Guidelines § 5.1 (Privacy) (2024), https://developer.apple.com/app-store/review/guidelines/.
[24] Google LLC, Google Play Developer Policy Center: User Data (2024),

ISSN: 2582-6433

distributing applications outside official stores—further limits the effectiveness of platform-level governance.

Efforts to promote international harmonisation have included the OECD Guidelines on Privacy, the APEC Cross-Border Privacy Rules system, and various bilateral data-sharing arrangements. These initiatives have generated useful normative frameworks, but they fall short of binding international law and have not resolved the fundamental tensions between divergent regulatory philosophies.[25]

The Council of Europe's Convention 108+, which extends data protection obligations to signatory states beyond Europe, offers a partial model for the elaboration of international minimum standards. A tiered regulatory architecture—in which binding international minimum standards coexist with more stringent national and regional requirements—may represent the most practicable path toward harmonisation, consistent with the legitimate interests of states in preserving regulatory autonomy over matters of national security and public order.

VI. REFORM PROPOSALS

A. Adaptive and Technology-Responsive Regulatory Frameworks

Regulatory frameworks must be designed to evolve with the technologies they govern. Static, prescriptive legislation is unsuited to a domain characterised by rapid and discontinuous innovation. Regulators should adopt principles-based governance supplemented by regularly updated technical guidance, and should expand the use of regulatory sandboxes to encompass AI-driven and blockchain-based mobile applications. Sunset clauses and mandatory review periods should be incorporated into primary legislation governing digital technologies to ensure periodic reassessment in light of technological change.[26]

B. Mandatory Algorithmic Transparency and Auditability

Mobile applications that employ AI or ML in decisions materially affecting users' rights or interests should be subject to mandatory algorithmic transparency requirements. Developers should be required to disclose, in accessible terms, the nature and basis of automated decisions,

https://play.google.com/about/developer-content-policy/.

[25] Asia-Pacific Economic Cooperation, APEC Cross-Border Privacy Rules System (2011), https://www.apec.org/groups/committee-on-trade-and-investment/electronic-commerce-steering-group/cross-border-privacy-rules-system.

ISSN: 2582-6433

and to maintain documentation enabling regulatory audit. Independent algorithmic audit regimes, modelled on financial audit frameworks, should be established to assess compliance with fairness and non-discrimination standards. The right to explanation under the GDPR should be given broader substantive content and more effective enforcement.[27]

C. Reconceptualising User Consent

The notice-and-consent model, in its current form, has failed as a mechanism for protecting user privacy in the context of AI-driven data processing. Future regulatory frameworks should require dynamic, granular, and revocable consent mechanisms, enabling users to specify the categories of data they are willing to share and to withdraw consent at any time without adverse consequence. Standardised, machine-readable privacy disclosures—replacing the current practice of lengthy, opaque privacy policies—should be mandated across jurisdictions. App stores should be empowered to enforce these requirements as a condition of distribution.[28]

D. A Legal Framework for Smart Contracts

The legal uncertainty surrounding smart contracts requires legislative attention. National legislatures should enact clear frameworks establishing the conditions under which smart contracts constitute legally enforceable agreements, the allocation of liability for coding errors and unforeseen contingencies, and the mechanisms available for dispute resolution. International efforts to develop model laws or conventions on the legal status of smart contracts—analogous to the UNCITRAL Model Law on Electronic Commerce—should be actively pursued.[29]

E. Strengthening KYC and AML Obligations for Blockchain Applications

Regulators should extend robust KYC and AML requirements to the developers and operators of blockchain-based mobile applications, including decentralised exchanges and peer-to-peer payment platforms. These requirements should be technologically neutral—focused on the function performed rather than the architecture employed—and should be

[27] European Commission, Proposal for a Regulation on a European Approach for Artificial Intelligence (Artificial Intelligence Act), COM (2021) 206 final (Apr. 21, 2021).
[28] L.H. Iwaya et al., E-Consent for Data Privacy: Consent Management for Mobile Health Technologies in Public Health Surveys and Disease Surveillance, in MEDINFO 2019: Health and Wellbeing e-Networks for All 1223, 1224–25 (2019).
[29] D. Patel et al., Towards Legally Enforceable Smart Contracts, in Blockchain–ICBC 2018, at 153, 155–57 (Springer 2018).

ISSN: 2582-6433

subject to cross-border enforcement cooperation. The Financial Action Task Force's guidance on virtual assets provides a useful starting point for the elaboration of international standards in this domain.

F. Building Regulatory Capacity and Technical Expertise

Governments should invest systematically in the technical capacity of regulatory institutions. This includes the creation of interdisciplinary technology advisory boards, the secondment of technical experts to regulatory agencies, and the development of specialised training programmes for legislative drafters and enforcement officials. Partnerships between regulatory bodies, universities, and civil society organisations can facilitate the ongoing exchange of knowledge necessary to keep regulation abreast of technological development.[30]

G. Pursuing International Minimum Standards

International organisations including the United Nations, the OECD, and the ITU should be charged with developing binding minimum standards for mobile application regulation, covering data privacy, algorithmic transparency, cybersecurity, and user consent. These standards should be designed to be compatible with more stringent national and regional frameworks, rather than displacing them. Inclusion of digital governance provisions in trade agreements could provide a further mechanism for promoting harmonisation and encouraging compliance.[31]

VII. CONCLUSION

The integration of Artificial Intelligence, Machine Learning, and Blockchain technology into mobile applications represents one of the defining regulatory challenges of the current period. These technologies expand the possibilities of digital commerce, communication, and service delivery; they also generate profound risks to privacy, autonomy, security, and the rule of law. Existing regulatory frameworks—designed for a less complex and less dynamic technological environment—are demonstrably inadequate to address these risks.

The reforms proposed in this article—adaptive governance, mandatory algorithmic transparency, reconceptualised consent mechanisms, legal clarity for smart contracts, enhanced

[30] ISO/IEC 27701:2019, Security Techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management (Int'l Org. for Standardization 2019).
[31] Council of Europe, Convention 108+ for the Protection of Individuals with Regard to the Processing of Personal Data (2018), https://www.coe.int/en/web/data-protection/convention108-and-protocol.

ISSN: 2582-6433

KYC obligations, investment in regulatory capacity, and the pursuit of international minimum standards—are not individually novel. What is novel is the urgency with which they must now be pursued, and the recognition that they must be pursued concurrently rather than sequentially. Piecemeal reform will not suffice. The scale and pace of technological change demand a comprehensive and anticipatory regulatory response.[32]

Effective regulation of mobile applications ultimately requires a shift in regulatory culture—from reactive rule-making triggered by scandal or crisis, to proactive, ethics-grounded governance that engages with technological complexity in real time. It requires legislatures and regulatory agencies that are technically literate, institutionally independent, and committed to the protection of user rights as a genuine regulatory objective rather than a rhetorical aspiration. The infrastructure of digital life is too consequential—and the people who depend on it too numerous—for anything less.

References:

Akpobome, O. The Impact of Emerging Technologies on Legal Frameworks: A Model for Adaptive Regulation. 5 Int'l J. Res. Pub. & Rev. 5046 (2024).

Asia-Pacific Economic Cooperation. APEC Cross-Border Privacy Rules System (2011).

Blaszczyk, M. Blockchain and Private Law (Jan. 2023) (unpublished manuscript), https://ssrn.com/abstract=4319649.

Cate, F.H. & Mayer-Schönberger, V. Notice and Consent in a World of Big Data. 3 Int'l Data Privacy L. 67 (2013).

Chesterman, Simon. Through a Glass, Darkly: Artificial Intelligence and the Problem of Opacity. 69 Am. J. Comp. L. 271 (2021).

Council of Europe. Convention 108+ for the Protection of Individuals with Regard to the Processing of Personal Data (2018).

Dwivedi, V. et al. Legally Enforceable Smart-Contract Languages: A Systematic Literature Review. 54 ACM Computing Surveys 1 (2021).

European Parliament and Council Regulation 2016/679, General Data Protection Regulation. 2016 O.J. (L 119) 1.

European Commission. Proposal for an Artificial Intelligence Act. COM (2021) 206 final.

Faguet, J.P. Decentralization and Governance. 53 World Dev. 2 (2014).

Giancaspro, M. Is a 'Smart Contract' Really a Smart Idea? Insights from a Legal Perspective.

ISSN: 2582-6433

33 Computer L. & Security Rev. 825 (2017).

Hoofnagle, C.J., van der Sloot, B. & Borgesius, F.Z. The European Union General Data Protection Regulation: What It Is and What It Means. 28 Info. & Commc'ns Tech. L. 65 (2019).

ISO/IEC 27701:2019, Security Techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management (2019).

Kannengiesser, N. et al. Challenges and Common Solutions in Smart Contract Development. 48 IEEE Transactions on Software Eng'g 4291 (2021).

Kavoliūnaitė-Ragauskienė, E. Artificial Intelligence in Manipulation: The Significance and Strategies for Prevention. 17 Baltic J. L. & Pol. 116 (2024).

Kuznetsov, O. et al. On the Integration of Artificial Intelligence and Blockchain Technology: A Perspective About Security. 12 IEEE Access 3881 (2024).

Marbouh, D. et al. A Blockchain-Based Regulatory Framework for mHealth. 7 Data 177 (2022).

Organisation for Economic Co-operation and Development. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013).

Patel, D. et al. Towards Legally Enforceable Smart Contracts. In Blockchain–ICBC 2018, 153 (Springer 2018).

Prince, A.E. & Schwarcz, D. Proxy Discrimination in the Age of Artificial Intelligence and Big Data. 105 Iowa L. Rev. 1257 (2019).

Wenhua, Z. et al. Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends. 12 Electronics 546 (2023).