Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 15s (2025)
https://www.jneonatalsurg.com

OPEN ACCESS

Cyber Security Laws In India - Constitutional Implications & Gaps

M. Lakshmana Kumar[1], P. Saleem Akram[2]

Koneru Lakshmaiah Education Foundation, (Deemed to be University), Guntur, A.P, India
Email ID: psaleemakram@gmail.com

Cite this paper as: M. Lakshmana Kumar, P. Saleem Akram, (2025) Cyber Security Laws In India - Constitutional Implications & Gaps. *Journal of Neonatal Surgery*, 14 (15s), 194-200.

ABSTRACT
This study critically examines cybersecurity laws in India, focusing on constitutional implications & and identified gaps within the existing legal system. The study delves into legislative developments, the role of government agencies, and the issues faced in implementing and enforcing these laws. In addition, it explores the delicate balance between ensuring national security and safeguarding digital rights. This article concludes with recommendations for legal reforms to enhance cybersecurity laws' efficacy. This analysis contributes to a nuanced understanding of India's evolving landscape of cybersecurity regulations. The landscape of cybersecurity laws in India presents a complex interplay of constitutional implications and notable gaps. This article delves into the constitutional structure guiding cybersecurity regulations, examining the balance between individual privacy rights and the State's responsibility to ensure national security. Key legislation, such as the Information Tech Act of 2000 and subsequent amendments, are analyzed considering constitutional principles. Despite strides, gaps persist in addressing emerging threats, cross-border challenges, and harmonizing legal provisions. This article outlines the nuanced legal terrain, emphasizing the need for a comprehensive, adaptive legislative approach to fortify India's cybersecurity structure in the face of evolving digital landscapes.

Keywords: *Cybersecurity Laws, Constitutional Implications, Legal system, Data Protection, Digital Rights.*

1. INTRODUCTION

In an age characterized by the omnipresence of technology, the importance of a comprehensive legal structure for cybersecurity in India becomes paramount. The digital transformation sweeping across sectors necessitates a safeguarding mechanism that protects sensitive information and upholds its citizens' constitutional rights. As the nation embraces the digital imperative, the legislative response must navigate the complex terrain of privacy, data protection, and national security, striking a delicate equilibrium between fostering innovation and ensuring resilience against cyber threats.

At the heart of India's cybersecurity laws lie constitutional principles that serve as guiding lights and potential sources of contention. The right to privacy, enshrined as a fundamental right by the Supreme Court, intertwines with the need for robust cybersecurity measures. Striking a balance between individual privacy and collective security becomes a constitutional tightrope walk. The constitutional foundations thus become a critical lens through which the efficacy and legitimacy of cybersecurity laws are assessed, creating a space where legal scholars and practitioners grapple with the evolving dynamics of tech constitutionalism.

India's legislative response to cybersecurity concerns has seen significant developments, including the Information Tech Act of 2000, & subsequent amendments. These legal instruments aim to address the intricacies of cyber threats, laying down provisions for data protection, electronic signatures, and offenses related to computer systems. However, with the rapidly evolving nature of cyber threats, tech often needs to catch up on legislative updates, leading to discernible gaps and challenges in enforcement. The legislative landscape, therefore, becomes a canvas where the brushstrokes of legal amendments must adapt to the dynamic contours of the digital canvas.

The implementation of cybersecurity laws in India is challenging. Regulatory challenges, ranging from the need for enhanced international cooperation to the efficient enforcement of cybercrime provisions, present notable gaps. As the digital domain transcends national borders, the effectiveness of cybersecurity laws depends on seamless collaboration and a shared understanding of the global cyber threat landscape. Identifying and addressing these regulatory challenges becomes imperative for a robust cybersecurity structure that aligns with the interconnected nature of cyberspace.

In recent years, the increasing digitization of various aspects of society has necessitated a robust legal system to address the evolving landscape of cyber threats in India. The introduction of cybersecurity laws reflects the nation's commitment to securing its digital infrastructure and safeguarding sensitive information. These laws aim to combat various cybercrimes,

including data breaches, hacking, and other malicious activities that threaten national security, economic stability, and individual privacy.

The enactment of several crucial laws and regulations has characterized India's legislative efforts in cybersecurity. The Information Tech Act of 2000 is the foundational statute governing electronic transactions addressing cyber offenses. Subsequent amendments and additional regulations have been introduced to keep pace with technological advancements and emerging cyber threats. This legislative system empowers law enforcement agencies and outlines legal procedures and penalties for those found guilty of cybercrimes.

The constitutional implications of cybersecurity laws in India are significant, as they intersect with fundamental rights guaranteed by the Constitution. Balancing the imperatives of national security and individual rights requires carefully examining constitutional principles. The right to privacy, freedom of speech, and protection against unreasonable searches and seizures are crucial elements that must be harmonized with the State's duty to secure its digital infrastructure. Striking this delicate balance is essential to ensure effective and constitutionally sound cybersecurity laws.

As India treads into the future, the evolution of cybersecurity laws becomes an ongoing saga. Balancing innovation with security, individual rights with collective well-being, and national interests with global collaboration will shape the contours of the legal system. The road ahead demands a proactive approach, encompassing continuous legislative updates, technological adaptation, and stakeholder engagement. Navigating this path requires a nuanced understanding of constitutional implications and a commitment to addressing the identified gaps, ensuring that the legal cybernetic maze is not just a deterrent but a catalyst for a secure, technologically resilient India.

2. CONSTITUTIONAL SYSTEM

India's cybersecurity landscape is intricately interwoven with its constitutional system, which provides the legal basis for addressing the evolving challenges in the digital realm. The Indian Constitution, framed in 1950, did not explicitly foresee the complexities of the cyber age. However, its resilience has allowed adaptations to safeguard citizens' rights amid technological advancements. Article 21, guaranteeing the right to life and personal liberty, forms the bedrock for privacy concerns in the digital domain. The judiciary has acknowledged privacy as a fundamental right, influencing cyber law policies.

Article 19(1)(a) ensuring the right to freedom of speech and expression has crucial implications for cybersecurity laws. The delicate balance between free expression and preventing cyber threats is evident in legal measures such as Section 66A of the Information Tech Act (2000), which faced constitutional challenges for being overly broad. Courts have struck down provisions that infringe upon freedom of expression, emphasizing the need for precision in drafting cyber laws to withstand constitutional scrutiny.

The directive principles enshrined in Article 40 promote the security of the state and the integrity of its institutions and guide legislative endeavors in cybersecurity. The Information Tech (Amendment) Act 2008 responded to global cyber threats aligned with constitutional principles. However, the rapid pace of technological evolution necessitates a continual reassessment of these laws to bridge emerging gaps.

Despite constitutional safeguards, gaps in India's cybersecurity legal structure persist. The absence of comprehensive data protection law until recently left citizens vulnerable. The Personal Data Protection Bill aims to address this void in the pipeline, reflecting a growing awareness of the constitutional imperative to protect individuals' informational autonomy. Striking the right balance between security and individual rights remains an ongoing constitutional challenge in India's cybersecurity landscape.

The constitutional implications of cybersecurity laws in India extend beyond fundamental rights to encompass the principles of federalism. India's federal structure has led to a shared responsibility between the central and state governments to implement cybersecurity measures. While the Union government legislates on critical aspects through acts like the Information Tech Act of 2000, states play a vital role in enforcement. This distribution of powers ensures a collaborative approach, reflecting the constitutional ethos of cooperative federalism in addressing cyber threats.

Article 73, conferring executive power on the Union in matters enumerated in the Union List, empowers the central government to legislate on communication technology. However, cybersecurity also involves subjects under the State List, necessitating cooperation. The constitutional mandate to foster inter-state cooperation under Article 256 becomes crucial in cybercrime, where coordinated efforts are indispensable.

The judiciary plays a pivotal role in shaping cybersecurity jurisprudence through its expansive interpretation of constitutional principles. The Supreme Court's landmark judgment in the Puttaswamy case, affirming the right to privacy, set a precedent for evaluating the constitutionality of cyber laws. Judicial activism ensures cybersecurity legislation aligns with constitutional norms, addressing potential overreach and safeguarding citizens' rights in the digital space.

While the constitutional structure provides a robust foundation, gaps arise from the rapid evolution of tech outpacing legal

developments. Cybersecurity challenges like data breaches and ransomware attacks highlight the need for dynamic legal responses. Balancing the imperative for stringent cybersecurity measures with preserving civil liberties presents an ongoing constitutional dilemma that necessitates constant legislative vigilance adaptation.

In conclusion, India's constitutional structure forms the cornerstone of its cybersecurity laws, influencing the delicate balance between individual rights, national security, and federal cooperation. The evolving nature of cyber threats underscores the importance of a responsive legal system that upholds constitutional principles while adapting to the complexities of the digital age.

Moreover, the constitutional mandate of a federal structure allocates specific powers and responsibilities among the central and state governments. This distribution of powers in cybersecurity influences the jurisdiction coordination of efforts to combat cyber threats. The concurrent jurisdiction over certain aspects of cybersecurity further emphasizes the need for collaboration and harmonization among central and state authorities to address the dynamic issues posed by cybercrimes.

The principle of the rule of law, another cornerstone of the constitutional system, underscores the necessity for clear, just laws governing cybersecurity. It demands that any legal provisions relating to cybersecurity are transparent, fair, and consistently enforced. The constitutional system, therefore, establishes the groundwork for developing robust adaptive cybersecurity laws that align with the evolving nature of cyber threats while safeguarding individual rights and upholding the rule of law. As tech advances, ensuring that cybersecurity laws remain constitutionally sound becomes crucial to maintaining India's secure, resilient digital environment.

3. LEGISLATIVE DEVELOPMENTS

In India, cybersecurity laws have undergone significant legislative developments to address the evolving digital landscape. The Information Tech Act of 2000 is the foundational legislation, but subsequent amendments and new acts have been introduced to tackle emerging cyber threats. The Personal Data Protection Bill of 2019 is crucial legislation addressing data security privacy concerns. However, there are constitutional implications regarding the right to privacy under Article 21, prompting ongoing discussions on striking the right balance between security and individual freedoms.

The Indian government introduced the National Cyber Security Policy in 2013 to establish a structure for addressing cybersecurity challenges comprehensively. This policy laid the groundwork for drafting the Data Protection Bill and the subsequent Personal Data Protection Act. These legislative efforts acknowledge the need for robust data protection mechanisms to align with global standards to safeguard citizens' privacy rights.

Currently in the legislative pipeline, the proposed Cyber Crime Bill aims to update and strengthen measures against cyber offenses. This includes provisions for enhanced penalties for cybercrimes, aligning with the ever-growing sophistication of cyber threats. The bill underscores the government's commitment to fortify the legal structure in response to the dynamic nature of cyber threats.

Despite these advancements, gaps in the legislative landscape persist. The absence of a comprehensive law addressing cyber warfare cyber terrorism poses a notable deficiency. The need for specific provisions for addressing cross-border cybercrime coordination mechanisms with international agencies is another area that requires attention. Addressing these gaps is essential for bolstering India's cybersecurity posture in an interconnected digital environment.

Constitutional implications arise from the intersection of cybersecurity laws and fundamental rights. Striking a balance between national security concerns and individual liberties, especially the right to privacy, remains an ongoing challenge. The judiciary plays a pivotal role in interpreting and reconciling these constitutional dimensions, ensuring that legislative measures align with the constitutional ethos.

In conclusion, India has made significant strides in bolstering its cybersecurity legal system, with legislative developments addressing data protection, cybercrimes, and national security. However, crucial gaps necessitate further attention to ensure a holistic, robust response to the evolving cyber threat landscape. Constitutional implications, particularly regarding the right to privacy, underscore the importance of careful legislative crafting to safeguard individual freedoms while upholding national security imperatives.

4. DATA PROTECTION & PRIVACY LAWS

India has witnessed a significant evolution in its cybersecurity legal system, marked by the introduction of various acts and bills. The Information Tech Act of 2000 forms the cornerstone, providing a legal foundation for electronic transactions addressing computer-related offenses. However, constitutional implications arise regarding balancing individual privacy rights with the State's duty to ensure national security. The right to privacy was affirmed as a fundamental right by the Supreme Court of India in the landmark judgment of Justice K.S. Puttaswamy (Retd.) v. Union of India in 2017, which emphasized the need for comprehensive data protection laws.

In response, the Personal Data Protection Bill of 2019 seeks to regulate the processing of personal data by various entities. It introduces the concept of a Data Protection Authority and defines principles such as consent, purpose limitation, and data

minimization. In addition, the bill incorporates provisions for the right to be forgotten and the right to data portability. The bill, though promising, has faced scrutiny for certain provisions, such as exemptions for government agencies and the absence of a robust enforcement mechanism.

Further constitutional implications arise with the Aadhaar (Targeted Delivery of Financial & Other Subsidies, Benefits & Services) Act, 2016. While it addresses the unique identification system, concerns linger regarding the balance between convenience and potential privacy threats. The Supreme Court's decision in the Aadhaar case struck a balance, upholding the use of Aadhaar for welfare schemes but limiting its scope for private entities.

Article 21 of the Indian Constitution, guaranteeing the right to life and personal liberty, intertwines with the evolving cybersecurity legal landscape. The judiciary plays a vital role in interpreting and safeguarding these constitutional rights in the context of emerging technologies. Section 66A of the Information Tech Act, which dealt with online speech, faced constitutional challenges and was eventually struck down by the Supreme Court in 2015 in the Shreya Singhal case.

Despite these legal developments, gaps persist. Comprehensive overarching legislation for data protection privacy needs to be clarified. While the Personal Data Protection Bill is a step forward, addressing concerns related to government surveillance, data localization, and cross-border data flows remains imperative. Striking an equilibrium between individual rights and national security will continue to shape India's cybersecurity legal landscape, necessitating continual adaptation and refinement of existing laws.

5. ROLE OF GOVERNMENT AGENCIES

Government agencies play a crucial role in implementing and enforcing cybersecurity laws. The Ministry of Electronics & Information Tech (MeitY) is at the forefront, formulating policies overseeing their execution. The National Cyber Security Coordinator of the Cyber Security Division focuses on strategic planning coordination, addressing gaps in the overall cybersecurity architecture.

The Cyber Crime Investigation Cell (CCIC) Cyber Crime Units (CCUs) across states are pivotal in enforcing cybersecurity laws. They investigate and prosecute cybercrimes, contributing significantly to deterring malicious activities. Strengthening these agencies with modern tools and training is essential to enhance their effectiveness.

Intelligence agencies such as the National Technical Study Organization (NTRO) and the Indian Computer Emergency Response Team (CERT-In) are proactive in cybersecurity. Their focus on preemptive measures, threat intelligence, and incident response contributes significantly to the nation's cybersecurity posture.

A cohesive approach involves collaboration between law enforcement agencies, intelligence bodies, and the private sector. Public-private partnerships, such as the National Cyber Security Partnership (NCSP), foster joint information-sharing efforts to combat cyber threats.

India actively participates in international collaborations due to the borderless nature of cyber threats. Engagements with organizations like INTERPOL's adherence to international cybersecurity conventions facilitate a global response to cybercrimes, reinforcing the nation's cybersecurity system.

6. INTERNATIONAL COLLABORATION & COMPLIANCE

Given the borderless nature of cyber threats, international collaboration compliance is a pivotal aspect of modern cybersecurity efforts. Nations worldwide increasingly recognize the need to work together to fortify their cyber defenses. Collaboration involves sharing intelligence on emerging threats, coordinating response strategies, and developing common standards for cybersecurity practices. In this interconnected digital landscape, no single country can insulate itself from cyber risks, making collaborative efforts essential to create a robust global defense against cyber threats.

One of the key issues in international collaboration is achieving compliance with diverse cybersecurity regulations across different jurisdictions. Nations often have varied legal systems, standards, and enforcement mechanisms, hindering seamless cooperation. Harmonizing these differences and establishing common ground for cybersecurity norms is crucial. Organizations such as INTERPOL forums like the Budapest Convention on Cybercrime play vital roles in fostering international collaboration by providing platforms for dialogue and facilitating the development of shared cybersecurity systems.

While collaboration is essential, it brings forth complex sovereignty, privacy, and data protection issues. Striking a balance among collective security measures respecting individual nations' legal autonomy is ongoing. Developing effective mechanisms for information sharing without compromising national interests or violating privacy rights is a delicate yet crucial task in promoting international cybersecurity cooperation.

In conclusion, the effectiveness of cybersecurity efforts on a global scale depends significantly on the willingness of nations to collaborate and comply with shared standards. As cyber threats evolve, a united front becomes imperative to address the issues malicious actors pose. International collaboration enhances the collective resilience against cyber threats and fosters

a safer, more secure digital environment for nations and their citizens.

7. ISSUES IN IMPLEMENTATION

Implementing cybersecurity laws in India faces multifaceted issues that hinder the effective enforcement of these regulations. One prominent obstacle is the rapid evolution of technology, which often outpaces the development of legislation. Cyber threats constantly evolve, making it challenging for existing laws to keep pace with emerging risks, resulting in potential gaps in the regulatory system. Consequently, authorities need help crafting and implementing laws that adequately address cyber threats' diverse and dynamic nature.

Another significant issue lies in the sheer complexity of cybercrimes. Cybersecurity incidents often span international borders, requiring coordinated efforts among nations. The lack of a harmonized global approach to cyber law enforcement poses issues in investigating and prosecuting cybercriminals, especially when they exploit jurisdictional loopholes. This complexity further exacerbates the difficulties Indian authorities face in effectively implementing and enforcing cybersecurity laws.

Resource constraints also contribute to issues in implementing cybersecurity laws. Adequate training, technological infrastructure, and skilled personnel are essential for law enforcement agencies to combat cyber threats effectively. However, limited resources may impede the ability of these agencies to keep pace with the evolving tactics of cybercriminals. This resource gap hampers the investigation resolution of cybercrimes, creating hurdles in implementing cybersecurity regulations.

Furthermore, public awareness education plays a crucial role in the success of cybersecurity laws. A lack of awareness among the general population regarding cybersecurity best practices and the potential consequences of cybercrimes can impede the reporting of incidents and hinder preventive measures. Addressing these issues requires a comprehensive approach that includes continuous legislative updates, international collaboration, resource allocation, and public awareness campaigns to strengthen the implementation of cybersecurity laws in India.

8. PROTECTION OF DIGITAL RIGHTS

Protecting digital rights is critical in the contemporary landscape of technological advancements. As individuals increasingly engage in online activities, concerns about the privacy and security of personal information have become paramount. Various countries, including India, have recognized the importance of safeguarding digital rights and have implemented legal systems to address these concerns.

In India, digital rights protection is enshrined in laws that aim to balance the need for cybersecurity with the preservation of individual liberties. The Information Tech Act, for instance, outlines provisions related to data protection, privacy, and the punishment of cybercrimes. However, the issue lies in striking the right balance between ensuring a secure digital environment and respecting the fundamental rights of citizens.

One of the key considerations in protecting digital rights is technology's evolving nature. As new technologies emerge, legal systems must adapt to address emerging threats and vulnerabilities. In addition, implementing these laws and regulations requires effective enforcement mechanisms to deter potential violations and provide recourse for individuals whose digital rights may be compromised.

9. CYBERSECURITY INCIDENTS & RESPONSE MECHANISMS

Cybersecurity incidents pose a significant threat in the modern digital landscape, encompassing various malicious activities such as data breaches, ransomware attacks, and denial-of-service incidents. As tech advances, so do the tactics employed by cyber adversaries, necessitating robust response mechanisms to mitigate the impact of these incidents. The first line of defense involves understanding the evolving nature of cyber threats and the vulnerabilities that cybercriminals exploit.

An effective response is crucial in a cybersecurity incident to minimize damages and prevent further compromise. Rapid identification and containment of the breach, coupled with thorough forensic analysis, is paramount. Government agencies, law enforcement, and private organizations orchestrate a coordinated response. Collaboration among these entities is essential for sharing threat intelligence, pooling resources, and collectively responding to sophisticated cyber attacks. In addition, public awareness campaigns and education initiatives enhance the overall cyber resilience of individuals and organizations.

Despite concerted efforts, issues persist in developing foolproof response mechanisms. These issues include cyber threats' sheer volume and complexity, resource constraints, and the need for continuous adaptation to emerging attack vectors. It is imperative for response strategies to be dynamic, incorporating the latest technologies and threat intelligence to stay ahead of cyber adversaries. Regular drills and simulations can bolster preparedness, allowing stakeholders to refine their response procedures to ensure a swift, coordinated reaction to cybersecurity incidents.

In conclusion, as the digital landscape evolves, the importance of robust cybersecurity incident response mechanisms cannot

be overstated. A proactive approach, combining technological innovation, inter-agency collaboration, and public engagement, is crucial to effectively mitigate the impact of cyber threats and safeguard the integrity of digital ecosystems.

10. RECOMMENDATIONS FOR LEGAL REFORMS

Several key recommendations for legal reforms are essential to address constitutional implications and fill gaps in India's cybersecurity legal system. First and foremost, there is a pressing need to harmonize cybersecurity laws with constitutional principles, ensuring they align with the fundamental rights guaranteed to citizens. This involves carefully reviewing legislation to ensure an appropriate balance between safeguarding national security and upholding individual freedoms.

A second crucial aspect involves enhancing collaboration among government agencies and stakeholders. Establishing clear lines of communication and cooperation mechanisms among various entities involved in cybersecurity is imperative. This collaborative approach can help in effective information sharing, coordination of response efforts, and overall improvement in the nation's cybersecurity posture.

In addition, the legal reforms should prioritize strengthening data protection privacy laws. Recognizing the increasing significance of personal data in cyberspace, amendments or additions to legislation should be made to bolster the protection of individual privacy rights. Stricter data handling, storage, and cross-border transfer regulations can contribute to a more robust and secure digital ecosystem.

Lastly, an ongoing commitment to regular updates and adaptability is crucial. Given the rapidly evolving nature of cyber threats, the legal system should be dynamic and capable of responding to emerging issues promptly. Establishing a mechanism for periodic review updates to ensure that laws stay current and effective in addressing the evolving cyber landscape will be essential for maintaining the resilience of India's cybersecurity legal infrastructure.

11. CONCLUSION

In conclusion, examining cybersecurity laws in India reveals a complex, evolving legal landscape that attempts to navigate the issues posed by the digital age. The constitutional implications underscore the delicate balance required to ensure the security of digital spaces while upholding fundamental rights. The legislative developments in this field demonstrate the government's recognition of the importance of robust cybersecurity systems, yet gaps and ambiguities persist, necessitating continual legal scrutiny reform.

Furthermore, the interplay between data protection privacy laws and cybersecurity regulations highlights the intricate relationship between safeguarding sensitive information and mitigating cyber threats. As the digital realm transcends national borders, the need for international collaboration becomes paramount. India's engagement with global cybersecurity standards and cooperation with other nations exemplifies the recognition that addressing cyber threats requires a collective, coordinated effort.

However, issues in implementation persist, ranging from resource constraints to the dynamic nature of cyber threats. As the frequency and sophistication of cyber incidents increase, there is a pressing need to fortify response mechanisms to ensure swift, effective action. In light of these observations, the recommendations for legal reforms emphasize the imperative of adapting and strengthening cybersecurity laws to meet the ever-evolving issues of the digital age. By addressing these concerns, India can foster a more secure, resilient digital environment that aligns with constitutional principles and global cybersecurity standards.

Declarations

Ethics approval:

This is an observational study; the data we represent here is the public domain data. Also, The Author confirmed that no ethical approval is required.

REFERENCES

[1] Chandrashekhar, S., & Behera, S. (2019). Cybersecurity in India: A legal perspective. International Journal of Cyber Criminology, 13(1), 23-42.

[2] Gupta, R., & Singh, A. (2020). Constitutional issues in implementing cybersecurity laws: A case study of India. Journal of Cybersecurity & Privacy, 1(2), 112-127.

[3] Ministry of Electronics & Information Technology. (2021). Information tech (Reasonable Security Practices & Procedures & Sensitive Personal Data or Information) Rules, 2011.

[4] Narayanan, S., & Menon, N. (2018). Data protection laws in India: Analyzing the implications on cybersecurity. International Journal of Law & Information Technology, 26(4), 345-369.

[5] Roy, A., & Agarwal, S. (2022). Cybersecurity governance in India: A critical analysis of legal & regulatory

systems. Journal of Information Privacy & Security, 18(1), 45-64.

[6] The Constitution of India. (1950).

[7] The Information Tech Act, 2000. (2000).

[8] The Personal Data Protection Bill, 2019. (2019).

[9] Unique Identification Authority of India. (2016). Aadhaar (Targeted Delivery of Financial & Other Subsidies, Benefits & Services) Act, 2016.

[10] Varshney, R., & Kapoor, M. (2017). Cybersecurity & constitutional implications: A study of gaps in Indian legal provisions. Journal of Cybersecurity, 2(1), 78-95.