Page 1655 – 1665 **DOI:** *https://doij.org/10.10000/IJLMH.1111624*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 2

2026

Digital Trauma and Victimology: Reforming BRICS Cyberlaws through the Lens of European Frameworks

KRISHRAJ SINGH SIKARWAR[1]

ABSTRACT

The rapid digitalization of the BRICS nations, namely Brazil, Russia, India, China, and South Africa, has produced extraordinary economic growth over the past decade. Yet this technological expansion has moved faster than the legal frameworks designed to protect the people living within it. Cyber legislation across these countries tends to revolve around national security, data localization, and the punishment of offenders. What it consistently fails to address is the profound psychological harm that falls on victims. This paper undertakes a comparative study of cyberlaws across the BRICS bloc, examining the specific statutory gaps that leave victims exposed to prolonged emotional and psychological suffering. Drawing on research into post-traumatic stress disorder, anxiety, identity-based trauma, and the unique features of digital victimization, the paper builds the case for urgent legislative reform. It then proposes that BRICS nations look to the European Union for guidance, specifically to the General Data Protection Regulation, the Network and Information Security Directive 2022/2555, and the Digital Services Act, as models for introducing trauma-informed legal remedies, mandatory psychological support, and direct victim compensation into their own systems.

Keywords: *BRICS, Cyberlaw, GDPR, European Union, Data Protection, Psychological Harm, Legal Reforms*

I. INTRODUCTION

The intersection of technology and human psychology is now producing legal challenges that traditional frameworks were simply never built to meet. The BRICS nations together account for a substantial share of the global population and an increasingly significant portion of world digital trade. As each of these countries has pushed its digital infrastructure outward, cybercrime has followed at pace. Ransomware, identity theft, financial fraud, and online harassment are no longer peripheral concerns. They sit at the centre of everyday digital life for hundreds of millions of people. And yet the injury that receives the least attention in law is often the most

[1] Author is a Student at Navrachana University, Vadodara, Gujarat, India.

 [ISSN 2581-5369]

enduring: the psychological wound that a serious cyber incident leaves behind.

Current cyber legislation in BRICS countries shares a structural tendency. The laws prioritize the protection of the state, critical infrastructure, and commercial data flows. They impose penalties on offenders and, in some cases, regulate how organizations collect and store personal information. What they rarely do is look squarely at the person sitting at the other end of the attack. When someone discovers their financial accounts have been drained, their identity stolen, or their most private images shared without consent, the question of how the legal system will support their recovery tends to go unanswered. That silence is itself a form of harm. A legal framework that responds to a serious violation by offering the victim nothing tangible communicates, even if unintentionally, that the suffering of the individual is secondary to other concerns.

This paper argues that BRICS nations must move toward humanizing their digital laws. Part II sets out the psychological evidence for why this matters, examining the clinical and sociological literature on what cybercrime does to its victims. Part III works through the five BRICS jurisdictions individually, identifying the specific legislative gaps that leave victims without adequate recourse. Part IV turns to the European Union, which has developed a suite of legal instruments that, while not without their own limitations, take the harm to individuals far more seriously than anything currently in place across the BRICS bloc. Part V draws that comparison into a set of practical reform recommendations. Part VI concludes with observations on what is at stake and a call for further research into the areas this paper identifies but cannot fully resolve.

II. THE PSYCHOLOGICAL TRAUMA OF CYBERCRIME VICTIMIZATION

To appreciate why legislative reform is so urgent, it is necessary to first take the psychological injury seriously as a medical and social fact. Victims of cybercrime do not merely suffer inconvenience or financial loss. They experience emotional and cognitive responses that, in many documented cases, are clinically indistinguishable from those triggered by physical assault or severe personal crisis. Research published in *BMC Public Health* in 2025 confirmed that cyberbullying victimization among young people produces measurable traumatic outcomes, including symptoms that meet diagnostic thresholds for trauma-related disorders.[2] The same patterns, with some variation in severity and mechanism, appear across adult populations subjected to financial fraud, data breaches, identity theft, and targeted harassment.

The particular character of digital crime compounds the harm in ways that traditional legal

[2] *Sameer Hinduja & Justin W. Patchin, Cyberbullying Through the Lens of Trauma: An Empirical Examination of US Youth*, 25 BMC Public Health (2025), DOI: 10.1186/s12889-025-22692-6, PMC12063437.

 [ISSN 2581-5369]

frameworks have not yet fully accounted for. In a conventional crime, the victim usually knows something concrete about what happened and who did it. In a cyberattack, the perpetrator is frequently invisible, anonymous, and potentially located in a different country. That anonymity removes any realistic prospect of confrontation or closure for many victims. What it leaves behind is a kind of ambient dread: an inability to feel safe at home, a changed relationship with personal devices, intrusive thoughts about who the attacker was and whether they will return.[3] The internet also preserves evidence of violation indefinitely. Images shared without consent, defamatory posts, or leaked personal data can resurface months or years after the initial incident, subjecting the victim to repeated re-traumatization over which they have almost no control.

Financial cybercrimes carry an additional dimension of harm. Investment scams, digital arrest frauds, and account takeovers frequently leave victims feeling ashamed as well as destitute. Social engineering works precisely because it exploits normal human trust, and victims tend to internalize that exploitation as personal failure. The resulting shame is a significant barrier to help-seeking, both from law enforcement and from personal support networks. People withdraw, isolate, and in the most serious cases, the combination of financial ruin and social humiliation has proven fatal.[4] When the legal system adds to this burden by offering nothing in the way of restitution or psychological support, it reinforces the victim's sense of abandonment and deepens the original wound considerably.

III. SYSTEMIC FLAWS IN BRICS CYBER LEGISLATION

Each of the five BRICS nations has made genuine legislative efforts in the cyber domain over the past decade. The problem is not that these laws are absent but that they are built around the wrong priorities. A careful reading of each jurisdiction reveals a consistent pattern: the state and its security interests occupy the centre of the legal frame, while the individual victim sits somewhere at the periphery, visible in the recitals and the policy statements but largely absent from the operative provisions that would actually help.

A. India: Removing the Right to Compensation

India's Digital Personal Data Protection Act of 2023 was introduced as a landmark piece of digital governance. The parliamentary debates and policy papers that accompanied it stressed the importance of protecting individuals and building trust in India's digital economy. In one critical respect, however, the Act moved sharply backward. Under the older Information

[3] *Miranda Bruce et al., Mapping the Global Geography of Cybercrime with the World Cybercrime Index*, 19(4) PLoS ONE e0297312 (2024), DOI: 10.1371/journal.pone.0297312, PMC11006133.

[4] *Malicious Life Podcast, Cyber PTSD*, Cybereason Blog (Mar. 28, 2022), https://www.cybereason.com/blog/malicious-life-podcast-cyber-ptsd.

 [ISSN 2581-5369]

Technology Act of 2000, Section 43A gave data breach victims a direct statutory right to claim compensation from corporate bodies that handled their sensitive personal data negligently.[5] That was an imperfect mechanism in many ways, but it was a genuine legal remedy pointing directly at the person who had suffered the harm.

The DPDPA abolished it. Under the new framework, the Data Protection Board can levy substantial penalties on non-compliant entities, penalties that can reach up to two hundred and fifty crore rupees in the most serious cases. Those penalties flow entirely into the Consolidated Fund of India.[6] The person whose health records, financial details, or biometric data were leaked receives nothing directly from that process. They are left to initiate their own civil litigation if they want any restitution, a path that is realistic only for those with significant resources and resilience. For the vast majority of victims, the DPDPA's penalty regime is simply irrelevant to their actual situation. The state collects the fine. The individual manages the fallout alone.

B. Russia: Surveillance, Opacity, and Deteriorating Digital Trust

Russia's approach to cyber governance is shaped overwhelmingly by state security objectives. The 2019 Sovereign Internet Law introduced a technical infrastructure that allows the state to centrally filter, reroute, and block internet traffic through Deep Packet Inspection technology installed across internet service providers. Human Rights Watch documented in 2025 how this system has been used to throttle services, block independent media, and isolate Russian internet users from significant portions of the global web.[7] The government's primary stated concern is protecting Russian digital infrastructure from foreign interference. The effect on ordinary citizens is a communications environment characterized by opacity, unpredictability, and an ever-present awareness of being watched.

The clinical literature on surveillance and mental health is relevant here. Research published in *Cureus* in 2024 examined the relationship between pervasive security technologies and psychological outcomes, finding consistent associations between chronic exposure to surveillance environments and elevated anxiety, behavioral inhibition, and self-censorship.[8] Alongside this structural anxiety, Russian citizens face a separate and equally serious problem: the state's surveillance apparatus does almost nothing to protect them from actual criminal

[5] Information Technology Act, No. 21 of 2000, s 43A (India).
[6] Digital Personal Data Protection Act, No. 22 of 2023, s 34 (India).
[7] *Human Rights Watch, Disrupted, Throttled, and Blocked: State Censorship, Control, and Increasing Isolation of Internet Users in Russia* (HRW, Jul. 30, 2025), https://www.hrw.org/report/2025/07/30/disrupted-throttled-and-blocked/state-censorship-control-and-increasing-isolation.
[8] *Adwait S. Malik et al., Exploring the Impact of Security Technologies on Mental Health: A Comprehensive Review*, 16(2) Cureus e53664 (2024), DOI: 10.7759/cureus.53664, PMC10918303.

 [ISSN 2581-5369]

hackers. The period from 2022 to 2024 saw a substantial escalation in the theft and public leakage of Russian personal databases, a trend documented by the Carnegie Endowment for International Peace in early 2026.[9] The result is a population navigating two overlapping threats simultaneously: an intrusive state and a permissive criminal environment. The psychological consequences of that combination are chronic rather than episodic.

C. Brazil: The Architecture Is Sound; the Execution Is Not

Brazil's General Data Protection Law, the LGPD, stands as probably the most philosophically coherent data protection statute among the BRICS nations. Modeled closely on the GDPR, it frames data protection as a fundamental right, establishes a dedicated regulatory body in the National Data Protection Authority, and allows victims to seek moral damages for breaches of their personal data rights. On paper, it is exactly the kind of human-centered framework this paper is arguing for.

The gap between paper and practice is where the difficulty lies. Jones Day's analysis of ANPD enforcement trends in September 2024 noted that enforcement has been accelerating, but the process of obtaining relief remains slow, expensive, and demanding for individual claimants.[10] Victims who can demonstrate psychological or moral harm from a data leak still face the prospect of protracted litigation to quantify and prove that harm. The burden sits on the most vulnerable party in the transaction. More troublingly, public sector entities in Brazil have been slow to comply with the LGPD, meaning the institutions that hold some of the most sensitive personal data, health records, tax information, welfare data, have remained among the least accountable. When the harm comes from the state itself, the victim's sense of betrayal adds a political dimension to the psychological injury that is particularly difficult to process.

D. China: State Primacy and the Absent Individual

China operates one of the most extensive and technically sophisticated cyber regulatory systems in the world. The Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law together create a dense, interlocking set of obligations on network operators and data handlers. Bird and Bird's 2026 analysis of the revised Cybersecurity Law documented how recent amendments have extended this framework to cover emerging areas including artificial intelligence governance, deepfake regulation, and algorithmic accountability.[11] The technical

[9] *Maria Kolomychenko, Russia's Cyberfraud Epidemic Is Now a Political Issue*, Carnegie Endowment for International Peace, Politika (Jan. 19, 2026), https://carnegieendowment.org/russia-eurasia/politika/2026/01/russia-cybersecurity-problems.

[10] *Jones Day, Brazil Amps Up Enforcement of Data Protection Law*, Jones Day Insights (Sept. 2024), https://www.jonesday.com/en/insights/2024/09/brazil-amps-up-enforcement-of-data-protection-law.

[11] *Bird & Bird, Key Revisions and Compliance Recommendations of the PRC Cybersecurity Law*, Bird & Bird

ambition of the system is not in question.

The problem is the framework's fundamental orientation. National security and social stability are not merely among the law's priorities; they are its organizing principle. Individual privacy interests are recognized in the PIPL but consistently yield to state interests when the two conflict. Victims of cyber fraud or deepfake manipulation can in principle pursue civil claims, but the state's response to cybercrime incidents tends to focus on punishing offenders or sanctioning platforms rather than on restoring the individual's sense of security, dignity, or financial position. Psychological support is not mentioned in the legal framework. Transparent victim engagement is not part of incident response protocols. The individual who has been harmed is treated, in practice, as a data point within a broader national security event.

E. South Africa: Institutional Fragmentation and Secondary Victimization

South Africa's two central instruments, the Protection of Personal Information Act and the Cybercrimes Act of 2020, contain substantively strong provisions. The Information Regulator has statutory independence and real enforcement powers. The Cybercrimes Act creates a comprehensive set of offences covering unlawful interception, malicious communications, and cyber extortion. The legislative foundation is adequate.

What is not adequate is the institutional capacity to deliver on what the law promises. The Information Regulator's own Annual Report for 2024/2025 details the backlogs and resource constraints that limit the speed and scale of its enforcement activity.[12] Cases involving security compromises pile up faster than they can be addressed. Victims wait. The psychological uncertainty of waiting for an institution to act on a violation of one's most private information is not a trivial burden. Beyond the regulator, law enforcement agencies frequently lack the specialized training to handle cybercrime victims sensitively. Reports of secondary victimization are not anecdotal. They are a pattern: victims of technology-facilitated gender-based violence, non-consensual image sharing, and online stalking describe encounters with police that range from dismissive to actively harmful.[13] A legal system that the victim finds unhelpful or unsafe is one that the victim stops using, and that non-reporting then makes accurate measurement of the problem impossible.

Insights (2026), https://www.twobirds.com/en/insights/2026/china/key-revisions-and-compliance-recommendations-of-the-prc-cybersecurity-law.

[12] *Information Regulator of South Africa, Annual Report 2024/2025* (InfoRegulator, 2025), https://inforegulator.org.za/wp-content/uploads/2025/11/Information-Regulator-Annual-Report-2025-210mm-x-260mm-1.pdf.

[13] *UN Women, Digital Violence in East and Southern Africa: Urgent Action Needed to Protect Women and Girls Online* (UN Women Africa, Nov. 2025), https://africa.unwomen.org/en/stories/press-release/2025/11/digital-violence-in-east-and-southern-africa-urgent-action-needed-to-protect-women-and-girls-online.

 [ISSN 2581-5369]

IV. MITIGATING TRAUMA: LESSONS FROM EUROPEAN CYBERLAWS

The European Union's approach to digital regulation is far from perfect. Implementation across member states is uneven, the GDPR's enforcement has been notoriously slow in several jurisdictions, and smaller entities routinely struggle with compliance burdens that were designed for large organizations. These criticisms are fair. But the EU's legislative instruments share an underlying premise that is largely absent from BRICS law: the premise that the harm to individual people matters in itself, and that the regulatory framework should be designed around that harm rather than simply around commercial or national security interests. That premise, more than any specific mechanism, is what BRICS legislators need to absorb.

A. Restoring Control: The GDPR Right to Erasure and Direct Compensation

One of the most practically significant features of the GDPR for victims of cybercrime is Article 17, the right to erasure. Where personal data is no longer necessary for its original purpose, where consent has been withdrawn, or where data has been unlawfully processed, the data subject can compel deletion.[14] For a victim of non-consensual image sharing, or someone whose personal details have been scraped and published by a malicious actor, the right to demand removal of that content from platforms and databases is psychologically as well as legally significant. It gives the victim an active role. The law stops treating them as a passive observer of their own violation and makes them a participant in ending it. The speed and accessibility of that right matter enormously in practice, but the principle is sound and BRICS nations should codify it.

Article 82 of the GDPR goes further by entitling any individual who has suffered material or non-material damage from a breach of the regulation to receive compensation directly from the controller or processor responsible.[15] Non-material damage explicitly includes psychological harm. India's decision to remove direct compensation from the DPDPA is therefore precisely the wrong direction of travel. A regulatory penalty that flows to the state treasury is a deterrence mechanism for the corporate sector. It is not a remedy for the person who was hurt. These are two different things, and conflating them leaves the victim without what the law owes them.

B. Speed and Transparency: The NIS2 Directive

The EU's NIS2 Directive addresses cybersecurity obligations for essential and important entities

[14] Regulation (EU) 2016/679 of the European Parliament and of the Council 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 (General Data Protection Regulation) [2016] OJ L 119/1, Art 17.
[15] Regulation (EU) 2016/679, Art 82.

 [ISSN 2581-5369]

across critical sectors. Among its core provisions is a strict incident notification timeline: a preliminary warning must be issued within twenty-four hours of a significant incident becoming known, with a full notification required within seventy-two hours.[16] The rationale for these timelines has a direct bearing on victim psychology. When organizations suppress or delay disclosure of a data breach, affected individuals have no opportunity to take protective action. They discover, sometimes months later, that their financial accounts have been compromised, their credentials sold on dark web markets, or their health information accessed. That discovery comes as a shock, compounded by the knowledge that they could have acted earlier if they had been told. Mandatory rapid notification does not eliminate harm, but it reduces the period of unknowing vulnerability and gives victims the agency to respond.

NIS2 also emphasizes the accountability of senior corporate management for cybersecurity governance and mandates continuous staff training and human resource security measures. The recognition that cybersecurity is a human organizational problem as much as a technical one is itself significant. Insider threats, negligent handling of credentials, and undertrained staff are responsible for a substantial portion of the incidents that ultimately harm end-users. A legal framework that pushes organizations toward sustained investment in security culture protects potential victims before the damage occurs.

C. Holding Platforms Accountable: The Digital Services Act

The Digital Services Act represents the most ambitious attempt yet to hold digital platforms directly responsible for the psychological environments they create. Under Articles 34 and 35, very large online platforms are required to conduct annual risk assessments covering a defined range of systemic risks, and to implement mitigation measures in response.[17] Critically, the list of systemic risks explicitly includes serious negative consequences for the physical and mental well-being of users. This is not aspirational language buried in a preamble. It is an operative legal obligation that platforms must demonstrate they have taken seriously.

The practical implications are considerable. Platforms are required to examine how their recommendation algorithms, user interface choices, and content moderation decisions affect the psychological safety of their users. Infinite scroll design that fosters compulsive use, algorithmic amplification of content that targets and humiliates particular users, automated systems that allow coordinated harassment to persist unchecked: these are all matters that fall

[16] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity Across the Union (NIS2 Directive) [2022] OJ L 333/80, Art 23.
[17] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act) [2022] OJ L 277/1, Arts 34-35.

 [ISSN 2581-5369]

within the scope of a properly conducted DSA risk assessment. If BRICS nations adopted equivalent provisions, they would be taking a qualitatively different approach to digital harm, moving from the current model of reacting to individual incidents toward a proactive legal requirement to prevent the structural conditions that produce mass psychological injury.

V. RECOMMENDATIONS FOR BRICS LEGISLATIVE REFORM

The reforms proposed below are specific, grounded in the legislative comparison developed above, and intended to be achievable within existing constitutional and political frameworks. They do not require BRICS nations to replicate EU law wholesale. They require those nations to take the psychological harm of their citizens seriously enough to build it into the architecture of their cyberlaws.

First, each BRICS nation should establish a statutory victim compensation fund. India provides the clearest current example of what goes wrong in the absence of one, but the gap exists across the bloc. Regulatory fines imposed on negligent data controllers should not disappear into general revenue. A defined portion, the precise percentage to be worked out through legislative process, should flow into a ring-fenced fund that makes direct payments to verified victims. This separates deterrence from remedy and ensures that the fine imposed on a corporation does not leave the individual it was meant to protect with nothing.

Second, mandatory training in trauma-informed practice should be introduced for cyber-related law enforcement and judicial officers. South Africa's experience with secondary victimization is not unique; it reflects a broader failure across BRICS jurisdictions to equip institutions with the tools to handle digital crime victims appropriately. Officers and prosecutors who understand the psychological dynamics of cybercrime, including why victims delay reporting, why they may be incoherent or inconsistent, and why shame and self-blame are predictable responses to certain kinds of digital violation, will produce better investigations and fewer instances of additional harm.

Third, an enforceable right to erasure should be codified across all five jurisdictions and applied with meaningful speed requirements. The right to remove oneself from a digital space where one has been violated is not a luxury. It is a precondition of recovery for many victims. The bureaucratic friction that currently characterizes most takedown and data deletion processes should be treated as a legal defect, not an acceptable administrative reality.

Fourth, the European Victims' Rights Directive model should be adapted for the cyber context. When an organization reports a significant data breach, part of that reporting obligation should include notification to affected individuals that includes not only a description of what happened

 [ISSN 2581-5369]

but also information about psychological support resources available to them. Incident response should not be purely a technical exercise. It should have a human communications dimension that addresses the affected person directly.

VI. Conclusion

Cyberspace is a social environment. The people who use it are not merely endpoints in a data network; they are human beings whose sense of safety, identity, and psychological integrity are bound up in their digital lives in ways that would have been inconceivable even twenty years ago. When that environment becomes a space where they can be robbed, humiliated, surveilled, or violated with limited legal consequence and no meaningful support from the state, the promise of digital development becomes something considerably darker.

The BRICS nations are not indifferent to this problem. Their legislators have made real efforts to regulate digital conduct, and several of the frameworks discussed in this paper contain genuine strengths. The difficulty is one of orientation. Laws built primarily to protect the state or punish offenders will always leave victims at the margins. The shift required is not technical. It is philosophical. It requires treating the psychological harm of the individual as a matter of legal concern in its own right, not as a secondary effect of a commercial or security failure.

The European Union's experience suggests that this shift is possible without abandoning the other legitimate goals of cyber regulation. The GDPR, NIS2, and the DSA all represent attempts, imperfect but serious, to build the harm to individuals into the structure of digital law rather than leaving it to chance litigation. BRICS nations that draw on those models, adapted to their own constitutional arrangements and social contexts, will produce legal frameworks that are not only more just but ultimately more effective. A digital citizen who trusts the legal system to support them is more likely to report crimes, cooperate with investigations, and participate openly in the digital economy. The case for reform is moral and practical in equal measure.

VII. Areas for further research

This paper has necessarily worked at a level of generality that leaves a number of important questions undeveloped. Several areas warrant dedicated scholarly attention. The first is empirical: there is a striking shortage of large-scale, longitudinal data on the psychological outcomes of cybercrime victimization specifically within BRICS populations. Most of the clinical literature on which this paper draws comes from North American or European study groups. Whether the patterns identified there translate directly to populations with different levels of institutional trust, digital literacy, and access to mental health services is an open

question that should be answered before legislative proposals are finalized. Second, the interaction between the compensation mechanisms proposed here and existing civil liability frameworks in each jurisdiction requires careful legal mapping. Simply mandating a victim fund without clarifying its relationship to tort claims, insurance recovery, and regulatory enforcement could produce inconsistent outcomes and create new litigation rather than reducing it. Third, the role of civil society organizations in delivering psychological support to cybercrime victims within BRICS contexts is underexplored. In several of the jurisdictions examined, NGOs and advocacy groups are currently filling gaps that formal legal frameworks have left open. Understanding how legislation can support and resource these organizations, rather than simply ignoring or duplicating their work, would make reform proposals more practical. Finally, comparative research into how trauma-informed principles have been embedded in victim support legislation outside the EU, particularly in jurisdictions closer in governance structure to BRICS members, could yield more directly applicable models than the European frameworks this paper has drawn on.

*****

 [ISSN 2581-5369]