Review of Futures Markets (RFM)
ISSN: 1933-7116
Volume 34 Issue 2 (2026)
Website: https://fra.st

Justice in the Cloud: Can Victims Cross the Digital Border? Bridging Victim Rights and Cross-Border Data Protection

Author: Shambhavi Gour
Research Scholar,
Amity University Haryana
shambhavi.gour2@gmail.com
Co-Author: Kratika Bhardwaj
Research Scholar,
Amity University, Haryana
kritikabhardwaj1915@gmail.com

Submission: 25.02.2025; Acceptance: 14.04.2025; Publication: 11.07.2026

Abstract
India stands at a constitutional inflection point where two ambitious legal projects the recalibration of criminal justice around the victim, and the construction of a modern data-protection regime have begun to intersect in ways that scholarship has yet to map. On 1 July 2024, the Bharatiya Nyaya Sanhita, 2023 (BNS), the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) and the Bharatiya Sakshya Adhiniyam, 2023 (BSA) replaced the colonial trinity of the Indian Penal Code, the Code of Criminal Procedure and the Indian Evidence Act, reorienting the system from a punitive, State-centred paradigm toward one that treats the victim as a rights-bearing stakeholder entitled to information, participation, compensation and dignity. Contemporaneously, the Digital Personal Data Protection Act, 2023 (DPDP Act) operationalised in phases from November 2025 alongside the Digital Personal Data Protection Rules, 2025 has erected a statutory architecture for informational privacy anchored in the Supreme Court's recognition of privacy as a fundamental right in K.S. Puttaswamy. This paper argues that these reforms are not parallel silos but converging vectors: the victim of the digital age is simultaneously a 'data principal' whose personal information traverses servers, jurisdictions and forensic pipelines. Adopting a doctrinal and comparative method, the study juxtaposes India's 'negative-list' model of cross-border transfer under Section 16 of the DPDP Act against the European Union's 'adequacy' architecture under Chapter V of the GDPR, and situates the victim at the fault line between investigative necessity and privacy protection. It concludes by proposing a victim-centric data-governance model reconciling dignity, due process and data sovereignty.
Keywords: victim-centric justice; Bharatiya Nagarik Suraksha Sanhita; Digital Personal Data Protection Act, 2023; cross-border data transfer; GDPR; informational privacy.

1. Introduction

The relationship between the individual and the State has always been most starkly revealed in the domain of criminal justice. For over a century and a half, that relationship in India was mediated by statutes drafted in a colonial idiom that conceived of crime as an offence against

the sovereign rather than an injury to a person. Within this architecture the victim was, at best, a witness for the prosecution and, at worst, a forgotten party whose suffering was instrumental to the State's vindication of its own authority. The reform wave that culminated on 1 July 2024 sought to invert this hierarchy, presenting justice rather than punishment as the organising value of the system.[1]

The three new codes did not merely rename their predecessors.[2] The Bharatiya Nyaya Sanhita renumbered and restructured the substantive law punishment for murder, once housed in Section 302, now appears as Section 101 while the Bharatiya Nagarik Suraksha Sanhita and the Bharatiya Sakshya Adhiniyam recast procedure and evidence for a digital era.[3] The very nomenclature of the procedural code 'Nagarik Suraksha', or protection of the citizen signalled an aspiration to a citizen-centric and victim-conscious system that balances the rights of the accused against those of the person wronged.

While the criminal codes were being rewritten, a second and initially unrelated transformation was unfolding in the law of information. In Justice K.S. Puttaswamy (Retd.) v. Union of India, a nine-judge bench of the Supreme Court unanimously held that the right to privacy is a fundamental right intrinsic to the guarantees of Articles 14, 19 and 21 of the Constitution.[4] That judgment rendered in the context of a global, information-based society expressly recognised informational privacy as a facet of the broader right, and directed the State to construct a robust data-protection framework.[5] The legislative answer arrived as the Digital Personal Data Protection Act, 2023, whose staggered commencement began with a notification dated 13 November 2025.

This paper proceeds from a simple but under-examined premise: the victim in a contemporary criminal proceeding is also a data subject. When a survivor of sexual violence lodges an electronic First Information Report, submits to audio-video recording of her statement, or has forensic evidence extracted from her devices, she generates a dense trail of intimate personal data. That data is stored, processed, indexed and in an internet-mediated world frequently transmitted across borders. The dignity that victim-centric reform seeks to restore is therefore inseparable from the informational privacy that data-protection law seeks to guarantee. The two projects meet most acutely at the frontier of cross-border data transfer, where investigative necessity, corporate cloud infrastructure and the sovereignty of the State collide.

---

[1] *Ministry of Home Affairs. (2024). New criminal laws: Features and implementation. Government of India.*

[2] K.I. Vibhute. (2024). *Bharatiya Nyaya Sanhita: A commentary*. Eastern Book Company.
Bhatia, G. (2024). India's new criminal laws: Reform or continuity? *Indian Law Review.*

[3] *Government of India. (2023). The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023). The Gazette of India.; Government of India. (2023). The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 46 of 2023). The Gazette of India.; Government of India. (2023). The Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023). The Gazette of India.*

[4] *Justice K. S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

[5] Committee of Experts under the Chairmanship of Justice B. N. Srikrishna. (2018). *A free and fair digital economy: Protecting privacy, empowering Indians*. Ministry of Electronics and Information Technology.

The scale of the criminal-law reform underscores its ambition. The Bharatiya Nagarik Suraksha Sanhita alone comprises five hundred and thirty-one sections against the Code of Criminal Procedure's four hundred and eighty-four, introducing fresh provisions, amending scores of others and deleting the obsolete, all in the service of a system reoriented toward speedy trial, effective justice and the protection of the citizen.[6] Yet ambition is not achievement. Whether these codes deliver on their victim-centric promise will depend on infrastructure, training and this paper contends on their coherence with the parallel data-protection regime, since a justice process that empowers the victim while leaking her sensitive data would betray the very dignity it professes to restore.

The paper examines the intersection of India's victim-centric criminal justice framework and cross-border data protection in an increasingly digital criminal justice ecosystem. It explores the evolution of victim rights in Indian criminal jurisprudence alongside the constitutional recognition of informational privacy, before analysing how the victim-centric provisions of the new criminal laws generate, process, and share sensitive personal data. The study further evaluates the relationship between India's Digital Personal Data Protection Act, 2023 and the European Union's General Data Protection Regulation (GDPR), with particular emphasis on their contrasting approaches to cross-border data transfers and the implications for transnational criminal investigations. Against the backdrop of cybercrime and cross-border evidence gathering, the paper argues for a victim-centric model of data governance that reconciles effective criminal justice with robust data protection. The study adopts a doctrinal and comparative methodology, drawing upon legislation, judicial decisions, and contemporary scholarly literature, while treating the European framework as a persuasive point of comparison rather than a model for direct transplantation.

2. Conceptual Foundations: Dignity, Victimhood and Informational Privacy

2.1 The Ascent of the Victim in Indian Criminal Justice

The marginality of the victim under the Code of Criminal Procedure, 1973 was structural rather than accidental. Prosecution was a contest between the State and the accused, in which the injured party possessed neither a defined status nor a voice at critical procedural junctures. It was only through the 2008 amendment that a statutory definition of 'victim' entered the Code, expansively encompassing any person who suffered loss or injury by reason of the act or omission charged, together with their guardian and legal heir. Even then, participatory rights remained thin: the victim could observe but rarely intervene, and could seldom compel the machinery of investigation to account for its lapses.

The theoretical foundation of the victim-centric turn is the recognition that a crime injures a concrete person whose autonomy, security and dignity have been violated, and that the criminal process owes that person more than the vicarious satisfaction of a conviction. Restorative and participatory theories of justice reframe the victim as a stakeholder with legitimate interests in

[6] Government of India. (2023). *The Bharatiya Nagarik Suraksha Sanhita, 2023* (Act No. 46 of 2023). *The Gazette of India.*

information, in being heard, and in reparation.[7] The Bharatiya Nagarik Suraksha Sanhita operationalises this philosophy by retaining and broadening the definition of victim under Section 2(1)(y) to include dependents and legal heirs, thereby extending participatory and compensatory entitlements beyond the directly injured individual.[8] The result is a normative shift from the victim as passive instrument to the victim as active participant a shift whose full realisation depends, as later parts show, on institutional capacity and on the protection of the victim's own personal data.

2.2 Privacy as a Constitutional Value: The Puttaswamy Turn

If victimhood supplies one axis of this study, informational privacy supplies the other. Before 2017, the constitutional status of privacy was contested, with earlier benches in M.P. Sharma and Kharak Singh having doubted its existence as a guaranteed right. Puttaswamy swept away that doubt, locating privacy within the inviolable core of personal liberty while acknowledging that the right is not absolute.[9] Crucially, the Court articulated a tripartite test for any State interference: the action must rest on a valid legal basis (legality), pursue a legitimate State aim (necessity), and be proportionate to that aim, adopting the least intrusive available means.

The judgment's significance for this paper lies in its treatment of informational privacy as an interest in preventing information about the self from being disseminated and in retaining a measure of control over one's personal data. That constitutional recognition catalysed the legislative process beginning with the Justice B.N. Srikrishna Committee's draft bill that eventually produced the DPDP Act.[10] The proportionality standard is not a doctrinal ornament; it is the analytical bridge between the two halves of this study. When the criminal process collects, retains and transfers a victim's data in the name of investigation, that collection is a privacy intrusion that must satisfy the Puttaswamy triad. Victim-centric justice, properly understood, therefore cannot be indifferent to data protection: to protect the victim is also to protect her information.

3. The New Criminal-Law Architecture and Its Victim-Centric Reorientation

3.1 Participation, Compensation and Care under the BNSS and BNS

The BNSS translates the rhetoric of victim-centrality into an interlocking set of enforceable rights. The right to information is strengthened at three points: the victim is entitled to a free copy of the First Information Report, must be apprised of the progress of the investigation within ninety days under Section 193(3), and must be supplied without delay and no later than

[7] Doak, J. (2008). *Victims' Rights, Human Rights and Criminal Justice.* Hart Publishing.; Christie, N. (1977).; Conflicts as property. *British Journal of Criminology, 17*(1), 1–15.; Van Ness, D., & Strong, K. (2015).

[8] Government of India. (2023). *The Bharatiya Nagarik Suraksha Sanhita, 2023* (Act No. 46 of 2023). *The Gazette of India.*

[9] *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.; *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.; *Justice K. S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

[10] Committee of Experts under the Chairmanship of Justice B. N. Srikrishna. (2018). *A free and fair digital economy: Protecting privacy, empowering Indians*. Ministry of Electronics and Information Technology.; Government of India. (2023). *Digital Personal Data Protection Act, 2023* (Act No. 22 of 2023). *The Gazette of India.*

fourteen days with the police report and connected documents under Section 230.[11] Participation is deepened by the requirement that the victim be heard before a public prosecutor may withdraw from a prosecution, a proviso that recognises the victim as a genuine stakeholder in the disposition of the case.

Compensation and care form the second pillar. Section 396 obliges every State Government, in coordination with the Centre, to formulate a victim-compensation scheme funded by the State, and permits interim relief while inquiry is pending, so that essential support is not deferred until the conclusion of proceedings.[12] Section 397 mandates that public and private hospitals furnish first aid and medical treatment, free of cost, to victims of specified sexual offences, while Section 398 requires every State to notify a witness-protection scheme.[13] The victim may also engage an advocate of choice to assist the prosecution, although the assisting role remains subordinate to that of the public prosecutor.[14] The Bharatiya Nyaya Sanhita reinforces this orientation through stricter, partly gender-neutral provisions on sexual violence, and the BNSS directs that the proceeds of crime, once attached, be distributed among victims converting confiscation into restitution.[15]

These provisions are significant, yet they are not unqualified. Commentators have noted that the richer information rights attach only where the victim is represented by an advocate, disadvantaging the socio-economically vulnerable, and that the compensation process, routed through Legal Services Authorities, adds a procedural layer that a direct judicial award might have avoided.[16] Civil-liberties observers have separately cautioned that the codes' expanded custodial and speech-related provisions carry countervailing risks to individual rights.[17] A victim-centric reading must hold these gains and gaps in view simultaneously.

3.2 Digitising Justice: e-FIR, Forensics and the Victim's Data Footprint

The most consequential feature of the new procedure, for present purposes, is its thorough digitisation. Section 173(1) permits information regarding a cognizable offence to be furnished orally or by electronic communication, institutionalising the electronic FIR and giving statutory footing to the 'Zero FIR' registrable at any police station irrespective of territorial jurisdiction that the Supreme Court had earlier endorsed in Lalita Kumari.[18] Section 173(3) introduces a fourteen-day preliminary enquiry for a defined band of offences, and Section 176 makes

[11] Government of India. (2023). *The Bharatiya Nagarik Suraksha Sanhita, 2023* (Act No. 46 of 2023). *The Gazette of India.*

[12] National Legal Services Authority. (2018). *Compensation Scheme for Women Victims/Survivors of Sexual Assault/Other Crimes, 2018*

[13] Supreme Court of India. (2018). *Witness Protection Scheme, 2018.*

[14] Government of India. (2023). *The Bharatiya Nagarik Suraksha Sanhita, 2023* (Act No. 46 of 2023). *The Gazette of India.*

[15] Government of India. (2023). *The Bharatiya Nyaya Sanhita, 2023* (Act No. 45 of 2023). *The Gazette of India.*

[16] Malimath Committee. (2003). *Committee on Reforms of Criminal Justice System*. Ministry of Home Affairs. Law Commission of India. (2009). *Report No. 226: The inclusion of victims' rights in the criminal justice system.*

[17] Amnesty International. (2024). *India: Authorities must immediately repeal repressive new criminal laws.*

[18] *Lalita Kumari v. Government of Uttar Pradesh*, (2014) 2 SCC 1.

forensic examination compulsory for offences punishable with seven years' imprisonment or more, requiring a forensic expert to visit the scene and to record the process.[19]

Each of these innovations multiplies the volume and sensitivity of personal data flowing through the justice system. Audio-video recording of statements, mandatory videography of search and seizure, electronic service of summons and the conduct of trials in electronic mode all generate durable digital records. Forensic mandates entail the extraction of biometric identifiers, device images and, potentially, genetic material; the enlarged power to collect finger impressions and voice samples under Section 349 extends even to persons not under arrest.[20] The victim, whose statement, medical record, forensic sample and identity documents enter this pipeline, becomes a prolific generator of sensitive personal data precisely the category that data-protection law exists to safeguard.

The codes are not oblivious to this tension. The Bharatiya Nyaya Sanhita retains, in Section 72, the offence of disclosing the identity of a victim of specified sexual offences, punishable with imprisonment and fine, thereby protecting the survivor from stigmatising publicity while permitting narrow, good-faith disclosures for investigation.[21] The BNSS correspondingly preserves in-camera trial and reporting restrictions for such offences under Section 366.[22] These are, in substance, sectoral data-protection norms embedded within criminal procedure. Their existence demonstrates that the drafters recognised the victim's informational dignity; their limits demonstrate why a general data-protection statute capable of governing storage, retention and, above all, cross-border transfer is indispensable to complete the protective architecture.

The digital reorientation is completed by Section 530 of the BNSS, which authorises trials, inquiries and proceedings including the recording of evidence and the service of summons to be conducted in electronic mode, and by the mandate that the forensic expert record the collection of evidence at the scene of serious crimes.[23] The consequence is that a victim's testimony, cross-examination and identity may now be captured, transmitted and archived as electronic records that persist indefinitely and can be duplicated at negligible cost. The admissibility of such records turns on statutory certification, but their protection turns on data-protection discipline; the two requirements, evidentiary and privacy-related, must be satisfied together if the digitised process is to serve rather than endanger the victim it was designed to empower.

[19] National Forensic Sciences University. (2023). Analysis of the Bharatiya Nagarik Suraksha Sanhita, 2023: Strengthening Scientific Investigation. Gandhinagar.

[20] Government of India. (2023). *Digital Personal Data Protection Act, 2023* (Act No. 22 of 2023). *The Gazette of India.;* Kerr, O. S. (2005). Digital Evidence and the New Criminal Procedure. Columbia Law Review, 105(1), 279–318.*;* Kuner, C. (2020). Transborder Data Flows and Data Privacy Law (2nd ed.). Oxford University Press.

[21] Law Commission of India. (2000). 172nd Report on Review of Rape Laws.

[22] Government of India. (2023). The Bharatiya Nagarik Suraksha Sanhita, 2023. Section 366.

[23] Ministry of Home Affairs. (2023). Bharatiya Nagarik Suraksha Sanhita, 2023: Statement of Objects and Reasons.

4. India's Data-Protection Framework in Comparative Light

4.1 The Digital Personal Data Protection Act, 2023: Architecture and Ambitions

The DPDP Act supplies the general regime that criminal procedure presupposes. It regulates the processing of digital personal data through a consent-centred model built around two principal actors: the Data Principal, to whom the data relates, and the Data Fiduciary, who determines the purpose and means of processing. The Act confers rights of access, correction and erasure, imposes obligations of purpose limitation, security safeguards and breach notification, and establishes a Data Protection Board to adjudicate contraventions. Its enforcement teeth are formidable: penalties for serious breaches or failures to safeguard personal data may reach two hundred and fifty crore rupees.[24]

Two features are especially salient for the victim-as-data-principal. First, the Act carries forward the constitutional lineage of Puttaswamy, translating the abstract right to informational privacy into concrete statutory entitlements and, in limited form, gesturing toward a right to erasure that resonates with the emergent 'right to be forgotten' recognised piecemeal by Indian courts and squarely codified in the European Union.[25] Second, the Act does not operate in a vacuum: the Information Technology Act, 2000 continues to penalise breach of confidentiality and unlawful disclosure of personal information under Sections 72 and 72A, and the Information Technology (Sensitive Personal Data) Rules, 2011 will remain operational until the DPDP regime is fully commenced.[26] Importantly, the Act exempts from several obligations processing undertaken for the prevention, detection, investigation or prosecution of offences an exemption that directly implicates the victim's data within the criminal process and to which Part 6 returns.[27]

The Act's operative logic rests on notice and consent: a Data Fiduciary must ordinarily furnish the Data Principal with an intelligible notice of the personal data sought and the purposes of processing, and must obtain a free, informed, specific and unambiguous consent that the Principal may withdraw. Around this core the statute arranges heightened duties for Significant Data Fiduciaries, safeguards for the personal data of children, and a grievance-redressal and adjudicatory apparatus centred on the Data Protection Board of India. For the victim-as-data-principal, however, the consent paradigm sits uneasily with the compulsions of a criminal investigation, where data is frequently gathered under legal authority rather than voluntary

[24] Justice B. N. Srikrishna Committee. (2018). A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians. Ministry of Electronics and Information Technology.; Greenleaf, G. (2024). Global Data Privacy Laws 2024: DPDP Act and International Comparisons. Privacy Laws & Business International Report

[25] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 ; Government of India. (2023). Digital Personal Data Protection Act, 2023.; Koops, B. J. (2011). Forgetting Footprints, Shunning Shadows: A Critical Analysis of the Right to Be Forgotten. SCRIPTed, 8(3), 229–256.

[26] Government of India. (2000). Information Technology Act, 2000. Sections 72 & 72A.; Government of India. (2011). Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011; Ministry of Electronics and Information Technology. (2023). Digital Personal Data Protection Act, 2023.

[27] Government of India. (2023). Digital Personal Data Protection Act, 2023. Section 17; Justice B. N. Srikrishna Committee. (2018). A Free and Fair Digital Economy.

agreement. This is precisely why the statutory exemptions for law-enforcement processing must be read narrowly and disciplined by proportionality, lest the consent architecture that protects the ordinary data principal evaporate for the victims and survivors whose data is most sensitive and most exposed.

4.2 The GDPR Benchmark: Rights, Accountability and Enforcement

The European Union's General Data Protection Regulation furnishes the global benchmark against which the DPDP Act is inevitably measured. The GDPR rests on a richer taxonomy of lawful bases than consent alone, imposes accountability and data-protection-by-design obligations, and confers an extensive suite of data-subject rights including access, rectification, portability and erasure under Article 17. Its extraterritorial reach and its penalty ceiling up to four per cent of global annual turnover have made it the de facto reference point for privacy regulation worldwide.[28]

The comparison is instructive precisely because the two instruments diverge in emphasis. Where the GDPR distinguishes ordinary from 'special category' data and layers heightened protections onto the latter, the DPDP Act adopts a flatter structure that does not formally tier sensitivity, leaving such gradation to sectoral regulators.[29] Where the GDPR embeds transfer discipline into a detailed statutory chapter, the DPDP Act delegates the question of cross-border movement to executive notification. These architectural choices are not merely technical; they shape how robustly a victim's sensitive data her medical history, sexual history and biometric identifiers will be shielded once it leaves the investigating agency's immediate control. The contrast becomes sharpest, and most consequential, in the law of cross-border transfer, to which the analysis now turns.

5. Cross-Border Data Transfer: Divergent Regulatory Philosophies

5.1 The GDPR's Whitelist: Adequacy, Safeguards and the Schrems Legacy

Chapter V of the GDPR erects a presumptive prohibition. Article 44 forbids the transfer of personal data to a third country unless one of a hierarchy of mechanisms applies.[30] At the apex sits the adequacy decision under Article 45, by which the European Commission certifies that a destination provides essentially equivalent protection; adequacy currently extends to roughly fifteen jurisdictions.[31] Absent adequacy, exporters must rely on 'appropriate safeguards' under Article 46 principally Standard Contractual Clauses (SCCs) and, for intra-group transfers, Binding Corporate Rules under Article 47 or, in narrow cases, the derogations of Article 49.

---

[28] European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation).
Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer.; Kuner, C., Bygrave, L. A., & Docksey, C. (Eds.). (2020). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press.

[29] European Union. (2016). General Data Protection Regulation. Article 9.

[30] European Union. (2016). General Data Protection Regulation. Chapter V; Article 44.;
Kuner, C. (2020). Transborder Data Flows and Data Privacy Law (2nd ed.). Oxford University Press.

[31] European Union. (2016). General Data Protection Regulation. Article 45.;
European Commission. (2024). Adequacy Decisions: How the EU Determines Equivalent Data Protection.

This architecture has been forged in litigation. In Schrems II the Court of Justice invalidated the EU-US Privacy Shield and held that reliance on SCCs alone is insufficient, requiring exporters to conduct a Transfer Impact Assessment (TIA) evaluating the destination's surveillance laws a requirement operationalised through the European Data Protection Board's Recommendations 01/2020.[32] The enforcement stakes were underscored when Meta was fined 1.2 billion euros in 2023 for unlawful transatlantic transfers.[33] The transatlantic breach was provisionally healed by the EU-US Data Privacy Framework, adopted by adequacy decision in July 2023 on the strength of United States Executive Order 14086 and its new Data Protection Review Court, permitting flows to self-certified US organisations.[34] Yet the framework's durability is contested; anticipating a possible 'Schrems III' challenge, cautious controllers retain SCCs and TIAs as fallback mechanisms.[35] A first review by the European Data Protection Board in 2024 endorsed the framework while urging continued vigilance.[36]

The instability of the transatlantic arrangement is best appreciated as a lineage of successive, judicially contested compromises: the Safe Harbour arrangement fell to the first Schrems challenge, its Privacy Shield successor to the second, and the present Data Privacy Framework has been characterised, not unfairly, as a 'Safe Harbour III' whose administration and monitoring echo its predecessors.[37] The July 2023 adequacy decision was expressly grounded

[32] Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems (Schrems II), Case C-311/18, Court of Justice of the European Union (2020).;
European Data Protection Board. (2021). Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data.;
European Data Protection Board. (2021). Recommendations 02/2020 on the European Essential Guarantees for Surveillance Measures.

[33] Data Protection Commission (Ireland). (2023). Decision in Inquiry into Meta Platforms Ireland Limited (Facebook EU-US Data Transfers). Dublin: Irish Data Protection Commission.;
European Data Protection Board. (2023). EDPB Binding Decision 1/2023 on the Dispute Submitted by the Irish Data Protection Commission Regarding Meta Platforms Ireland Limited.

[34] European Commission. (2023). Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 on the adequate level of protection of personal data under the EU–US Data Privacy Framework. Official Journal of the European Union, L231, 118–169.;
Executive Office of the President. (2022). Executive Order No. 14086 of October 7, 2022: Enhancing Safeguards for United States Signals Intelligence Activities. 87 Fed. Reg. 62283.;
U.S. Department of Commerce. (2023). EU–U.S. Data Privacy Framework Principles.

[35] European Data Protection Board. (2024). Opinion 28/2024 on Certain Data Protection Aspects Related to the EU–US Data Privacy Framework.;
Lynskey, O. (2024). "Schrems III?" The Future of EU–US Data Transfers after the Data Privacy Framework. Common Market Law Review, 61(5), 1339–1368.;
European Commission. (2021). Commission Implementing Decision (EU) 2021/914 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries.

[36] European Data Protection Board. (2024). Report on the First Review of the EU–US Data Privacy Framework.;
European Commission. (2024). Report from the Commission to the European Parliament and the Council on the First Periodic Review of the Functioning of the EU–US Data Privacy Framework.

[37] Maximillian Schrems v. Data Protection Commissioner (Schrems I), Case C-362/14, Court of Justice of the European Union (2015).;

in the redress guarantees introduced by Executive Order 14086, and its beneficial reach was understood to extend beyond self-certified importers to reassure those relying on Standard Contractual Clauses and Binding Corporate Rules.[38] The lesson for India is cautionary as much as exemplary: a rights-first transfer regime buys strong protection but tethers cross-border commerce to the shifting adequacy assessments of courts and commissions, generating recurrent legal uncertainty that a negative-list model largely avoids at the cost of a correspondingly weaker guarantee of protection abroad.

5.2 India's Blacklist: Section 16, Rule 15 and the Sovereignty Calculus

India has chosen the mirror image of the European model. Section 16 of the DPDP Act permits the transfer of personal data to any country or territory except those the Central Government notifies as restricted a 'negative-list' or blacklist approach that inverts the GDPR's adequacy-based whitelist.[39] Rule 15 of the DPDP Rules, 2025 operationalises this framework, and the staggered notification of 13 November 2025 confirmed a phased commencement in which the cross-border provisions are slated to take effect on 13 May 2027.[40]

The practical consequences are considerable. Because transfers are permitted by default until a restriction is notified, and because no restricted-country list had been issued as of mid-2026, cross-border flows are presently broadly lawful, subject to the general obligations that continue to bind the exporting fiduciary regardless of destination.[41] The Act deliberately declines to import the GDPR's transfer machinery: it does not, of its own force, require SCCs, Binding Corporate Rules or Transfer Impact Assessments, and any effort to retrofit those constructs onto Indian law risks misdirecting compliance energy from the Act's actual requirement of a lawful processing basis.[42] The final statute also abandoned the strict data-localisation mandate of earlier drafts in favour of this more permissive posture, informed by a risk-tiered model canvassed in preparatory policy work.[43]

Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems (Schrems II), Case C-311/18, Court of Justice of the European Union (2020).;
Svantesson, D. J. B. (2024). Data Privacy Management, Cryptocurrencies and Blockchain Technology. Wolters Kluwer. (Discusses the evolution from Safe Harbour to Privacy Shield and the Data Privacy Framework.)

[38] European Commission. (2023). Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 on the adequate level of protection of personal data under the EU–US Data Privacy Framework.;
Executive Office of the President. (2022). Executive Order No. 14086 of October 7, 2022: Enhancing Safeguards for United States Signals Intelligence Activities.;
European Data Protection Board. (2023). Information Note on Data Transfers under the GDPR Following the Adoption of the EU–US Adequacy Decision.

[39] European Parliament & Council. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union, L119, 1–88.

[40] Ministry of Electronics and Information Technology. (2025). Digital Personal Data Protection Rules, 2025.

[41] Government of India. (2023). Digital Personal Data Protection Act, 2023.

[42] Greenleaf, G. (2024). Global Data Privacy Laws 2024: Despite Problems, 178 Laws Show GDPR Dominance. Privacy Laws & Business International Report.

[43] Committee of Experts under the Chairmanship of Justice B. N. Srikrishna. (2018). A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians; Ministry of Electronics and Information Technology. (2019). The Personal Data Protection Bill, 2019.

The negative-list design encodes a distinct regulatory philosophy. Rather than assessing the abstract adequacy of a destination's privacy law, it reserves to the executive a dynamic, geopolitically responsive power to restrict flows to jurisdictions deemed hostile, insecure or surveillance-prone, reportedly weighing inadequate protection, adversarial relations and state-surveillance practices.[44] This flexibility is purchased at the price of predictability: a friendly state with weak privacy law may remain open, while a well-regulated rival may be closed. Two qualifications temper the apparent liberalism of the regime. First, sectoral localisation persists and prevails: the Reserve Bank of India's 2018 circular confines payment-system data to servers in India, and comparable directions bind securities-market data.[45] Second, the Act preserves the possibility of restricting specified categories of data handled by Significant Data Fiduciaries. The upshot is a sovereignty-conscious model that privileges executive discretion and national-security considerations over the rights-first, judicially policed adequacy calculus of the European Union.

From an industry vantage, the negative-list architecture vests in the Central Government an exclusive power to 'blacklist' destinations by notification, so that transfers remain permissible to every jurisdiction save those expressly banned.[46] This confers welcome operational freedom on data fiduciaries, but it also transfers the locus of protection from an ex ante legal test to an ex post political judgment. For the victim whose data is at stake, the difference is material: under the European model a destination must affirmatively demonstrate adequacy before her data may flow there, whereas under the Indian model her data may flow freely until the executive, for reasons that need not centre on privacy at all, decides otherwise. A victim-centric reading therefore urges that, at least for the sensitive categories of victim data, the general permissiveness of Section 16 be supplemented by sectoral safeguards and by contractual discipline that survive the absence of a formal statutory mandate.

6. The Convergence Zone: Protecting Victim Data Across Borders

6.1 Transnational Cybercrime, Digital Evidence and the Displaced Victim

The two reform projects collide most forcefully in the investigation of transnational cybercrime, where the victim, the offender and the data may each reside in a different jurisdiction.[47] A citizen defrauded online in India may be targeted by a perpetrator abroad, using infrastructure whose server logs, subscriber records and forensic artefacts sit on cloud platforms in a third country. Under Indian law, such electronic records must satisfy the certification requirement of Section 65B of the Evidence Act (now mirrored in the BSA) to be

[44] Bhandari, V., & Eisen, M. (2024). India's Digital Personal Data Protection Act and Cross-Border Data Transfers. Computer Law & Security Review.

[45] Reserve Bank of India. (2018). Storage of Payment System Data (Circular DPSS.CO.OD.No.2785/06.08.005/2017-18).; Securities and Exchange Board of India. (2022). Cyber Security and Cyber Resilience Framework for Market Infrastructure Institutions.

[46] NASSCOM. (2023). Industry Analysis of the Digital Personal Data Protection Act, 2023.; CUTS International. (2023). The Digital Personal Data Protection Act, 2023: Implications for Businesses.

[47] Brenner, S. W. (2010). Cybercrime: Criminal Threats from Cyberspace. Praeger.; Wall, D. S. (2007). Cybercrime: The Transformation of Crime in the Information Age. Polity Press.

admissible, and access to foreign-held data ordinarily proceeds through slow Mutual Legal Assistance Treaties.[48]

International instruments have sought to compress these delays. The Council of Europe's Budapest Convention harmonises cybercrime offences, mandates expedited preservation of stored data, and functions as a limited mutual-assistance framework among its parties.[49] Its Second Additional Protocol, opened for signature in 2022, goes further, enabling direct cooperation with service providers for subscriber information, emergency assistance and joint investigation teams.[50] India, however, is not a party to the Budapest Convention, a non-alignment that constrains its access to these expedited channels and leaves it dependent on bilateral treaties and the emerging United Nations Convention against Cybercrime.[51] Parallel national instruments such as the United States CLOUD Act, together with a discernible global drift toward data localisation, further fragment the landscape.[52]

That the Budapest Convention remains, notwithstanding its age, the most comprehensive and coherent international agreement on cybercrime and electronic evidence and a global reference point for domestic legislation and cross-border cooperation sharpens the cost of India's abstention.[53] India's reservations are principled, resting on concerns about sovereignty and the privacy implications of direct foreign access to data held on its soil, and they inform its preference for a United Nations-led instrument. But the interregnum is not costless for victims: while diplomacy proceeds, survivors of transnational fraud, extortion and image-based abuse wait on mutual-assistance processes ill-suited to the velocity of digital evidence, and the personal data essential to their cases either languishes unpreserved or is shared through channels lacking harmonised safeguards. The victim's interest thus argues for cooperation frameworks that are at once faster and more protective a dual demand that neither pure sovereignty nor pure openness can satisfy alone.

For the victim, this fragmentation is not an abstraction. Delay in securing cross-border evidence prolongs the investigation and defers the compensation and closure that victim-centric reform promises; yet the same cross-border cooperation that accelerates redress also entails transmitting the victim's own sensitive data statements, financial records, images into jurisdictions whose protective standards may fall short of Indian or European norms. International cooperation frameworks have begun, belatedly, to foreground the protection of victims in cyberspace as a value coordinate with, and not subordinate to, effective

[48] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.; Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.; United Nations Office on Drugs and Crime. (2013). Comprehensive Study on Cybercrime.

[49] Council of Europe. (2001). Convention on Cybercrime (ETS No. 185).; Brown, C. D. (Ed.). (2021). Research Handbook on International Cybersecurity Law. Edward Elgar.

[50] Council of Europe. (2022). Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence.

[51] United Nations Office on Drugs and Crime. (2024). United Nations Convention against Cybercrime.; Ministry of External Affairs. (2022). India's statements during UN Ad Hoc Committee negotiations on cybercrime.

[52] Chander, A., & Lê, U. P. (2015). Data Nationalism. Emory Law Journal, 64(3), 677–739.

[53] United Nations Office on Drugs and Crime. (2013). Comprehensive Study on Cybercrime.

enforcement.[54] The victim thus stands simultaneously to benefit from, and to be endangered by, the very flows the two legal regimes govern.

6.2 Toward a Victim-Centric Data-Governance Model

Reconciling these imperatives requires reading the criminal codes and the data-protection statute as a single normative field disciplined by the Puttaswamy proportionality test. The DPDP Act's exemption for processing undertaken to prevent, detect, investigate or prosecute offences must not be read as a blanket licence; it should be construed as a proportionate carve-out, engaging only so much of the victim's data, transferred only so far, as the legitimate investigative aim genuinely requires.[55] Where a victim's sensitive data must cross a border for forensic analysis or evidence-sharing, the exemption's beneficiaries should nonetheless observe minimisation, purpose limitation and secure-transfer discipline, borrowing the substance if not the label of the Transfer Impact Assessment that European law makes mandatory.[56]

Four design principles follow. First, sensitivity-tiering: because the DPDP Act does not itself grade data by sensitivity, the categories of victim data most in need of protection sexual, medical, biometric and genetic should be shielded by sectoral rules and by the identity-protection provisions already embedded in the BNS and BNSS. Second, dignity by default: the statutory protection of victim identity under Section 72 of the BNS should extend, in spirit, to every downstream processor and cross-border recipient of that identity. Third, calibrated cooperation: India's eventual accession to a multilateral cybercrime framework, and the maturation of the DPDP restricted-list power, should be coordinated so that faster evidence-sharing does not outpace the safeguards that protect the victims whose cases depend on it. Fourth, remedial coherence: the victim-compensation and witness-protection schemes of the BNSS should account for informational harms re-victimisation through data breach or unlawful disclosure as compensable injuries, aligning the remedial logic of criminal procedure with the penalty architecture of the DPDP Act.

Such a model would neither subordinate privacy to security nor sacrifice enforcement to an absolutist reading of data protection. It would instead recognise that the victim's dignity, which animates the new criminal codes, and the data principal's informational autonomy, which animates the DPDP Act, are two expressions of the same constitutional commitment articulated in Puttaswamy. The negative-list model's executive flexibility can be reconciled with rights-protection if the discretion it confers is exercised transparently and proportionately; the criminal codes' digitisation can be reconciled with privacy if the data it generates is governed rather than merely gathered.

[54] United Nations Office on Drugs and Crime. (2023). Handbook on Justice for Victims.

[55] Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.; Aharon Barak. (2012). Proportionality: Constitutional Rights and Their Limitations. Cambridge University Press.

[56] European Commission. (2021). Commission Implementing Decision (EU) 2021/914 on Standard Contractual Clauses.

7. Conclusion

India has, within a single reform cycle, rewritten the grammar of its criminal justice system and erected the scaffolding of a modern data-protection regime. This paper has argued that these are not discrete achievements to be assessed in isolation, but interdependent components of a shared constitutional project rooted in human dignity. The victim whom the Bharatiya Nagarik Suraksha Sanhita seeks to empower through rights to information, participation, compensation and care is the same individual whom the Digital Personal Data Protection Act must protect as a data principal, and whose sensitive information, generated abundantly by a digitised justice process, now travels along cross-border pathways governed by radically different regulatory philosophies.

The comparison between the European Union's adequacy-based whitelist and India's notification-based blacklist is more than a taxonomic exercise. It reveals a genuine choice between a rights-first, judicially disciplined model and a sovereignty-first, executively administered one. Neither is costless: the former purchases protection at the price of rigidity and litigation, the latter purchases flexibility at the price of predictability and, potentially, of the victim's informational security. The task ahead is not to transplant one regime into the other, but to ensure that whichever pathway a victim's data travels, the proportionality standard of Puttaswamy accompanies it across the border.

As the DPDP cross-border provisions approach their 2027 commencement and India's posture toward multilateral cybercrime cooperation continues to evolve, the doctrinal space mapped here will only grow in practical importance. A victim-centric data-governance model one that treats informational harm as a species of victimisation, that reads investigative exemptions through the lens of necessity and proportionality, and that extends the dignity of the survivor to every server on which her data rests offers a principled route through this emerging terrain. Between the victim and the server lies not a void but a constitutional obligation; the coherence of India's two great reforms will be measured by how faithfully that obligation is honoured.

References

— Adjudicating and investigating cross-border cybercrimes: A study of India's jurisdictional framework. (2025). International Journal of Innovative Legal Research. https://ijirl.com
— Aharon Barak. (2012). Proportionality: Constitutional rights and their limitations. Cambridge University Press.
— Amnesty International. (2024, July 4). India: Authorities must immediately repeal repressive new criminal laws. https://www.amnesty.org/en/latest/news/2024/07/india-authorities-must-immediately-repeal-repressive-new-criminal-laws/
— Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
— Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
— Bhandari, V., & Eisen, M. (2024). India's Digital Personal Data Protection Act and cross-border data transfers. Computer Law & Security Review.
— Bhatia, G. (2024). India's new criminal laws: Reform or continuity? Indian Law Review.

— Brenner, S. W. (2010). Cybercrime: Criminal threats from cyberspace. Praeger.

— Brown, C. D. (Ed.). (2021). Research handbook on international cybersecurity law. Edward Elgar Publishing.
— Chander, A., & Lê, U. P. (2015). Data nationalism. Emory Law Journal, 64(3), 677–739.
— Christie, N. (1977). Conflicts as property. British Journal of Criminology, 17(1), 1–15. https://doi.org/10.1093/oxfordjournals.bjc.a046783
— Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115–141, 132 Stat. 1213 (2018).
— Committee of Experts under the Chairmanship of Justice B. N. Srikrishna. (2018). A free and fair digital economy: Protecting privacy, empowering Indians. Ministry of Electronics and Information Technology.
— Council of Europe. (2001). Convention on Cybercrime (ETS No. 185). https://www.coe.int/en/web/cybercrime/the-budapest-convention
— Council of Europe. (2022). Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. https://www.coe.int/en/web/cybercrime/the-budapest-convention
— Council of Europe. (2022). Explanatory report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence.
— Council of Europe. (2024). Budapest Convention on Cybercrime: Frequently asked questions. https://www.coe.int/en/web/cybercrime
— CUTS International. (2023). The Digital Personal Data Protection Act, 2023: Implications for businesses.
— Data Protection Commission. (2023). Decision in the inquiry into Meta Platforms Ireland Limited (Facebook EU–US data transfers). Dublin: Data Protection Commission.
— Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems (Schrems II), Case C-311/18, Court of Justice of the European Union, Judgment of 16 July 2020.
— Doak, J. (2008). Victims' rights, human rights and criminal justice: Reconceiving the role of third parties. Hart Publishing.
— European Commission. (2021). Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679. Official Journal of the European Union, L199, 31–61.
— European Commission. (2023). Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 on the adequate level of

protection of personal data under the EU–US Data Privacy Framework. Official Journal of the European Union, L231, 118–169.

— European Commission. (2024). Adequacy decisions: How the EU determines equivalent data protection. https://commission.europa.eu

— European Commission. (2024). Report from the Commission to the European Parliament and the Council on the first periodic review of the functioning of the EU–US Data Privacy Framework.

— European Data Protection Board. (2021). Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

— European Data Protection Board. (2021). Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

— European Data Protection Board. (2023). Binding Decision 1/2023 on the dispute submitted by the Irish Data Protection Commission regarding Meta Platforms Ireland Limited.

— European Data Protection Board. (2023). Information note on data transfers under the GDPR following the adoption of the EU–US adequacy decision.

— European Data Protection Board. (2024). Opinion 28/2024 on certain data protection aspects related to the EU–US Data Privacy Framework.

— European Data Protection Board. (2024). Report on the first review of the EU–US Data Privacy Framework.

— European Parliament and the Council. (2016). Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L119, 1–88.

— Executive Office of the President. (2022). Executive Order No. 14086 of October 7, 2022: Enhancing safeguards for United States signals intelligence activities. Federal Register, 87, 62283–62292.

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

— Government of India. (2009). The Code of Criminal Procedure (Amendment) Act, 2008 (Act No. 5 of 2009). The Gazette of India.

— Government of India. (2011). Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. The Gazette of India.

— Government of India. (2023). Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023). The Gazette of India.

— Government of India. (2023). The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 46 of 2023). The Gazette of India.

— Government of India. (2023). The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023). The Gazette of India.
— Government of India. (2023). The Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023). The Gazette of India.
— Government of India. (2025). Notification bringing provisions of the Digital Personal Data Protection Act, 2023 into force. The Gazette of India.
— Greenleaf, G. (2024). Global data privacy laws 2024: Despite problems, 178 laws show GDPR dominance. Privacy Laws & Business International Report.
— Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

— Kerr, O. S. (2005). Digital evidence and the new criminal procedure. Columbia Law Review, 105(1), 279–318.
— Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.
— Koops, B. J. (2011). Forgetting footprints, shunning shadows: A critical analysis of the "right to be forgotten." SCRIPTed, 8(3), 229–256.
— K.I. Vibhute. (2024). Bharatiya Nyaya Sanhita: A commentary. Eastern Book Company.
— Kuner, C. (2020). Transborder data flows and data privacy law (2nd ed.). Oxford University Press.
— Kuner, C., Bygrave, L. A., & Docksey, C. (Eds.). (2020). The EU General Data Protection Regulation (GDPR): A commentary. Oxford University Press.
— Lalita Kumari v. Government of Uttar Pradesh, (2014) 2 SCC 1.
— Law Commission of India. (2000). One hundred seventy-second report on review of rape laws (Report No. 172).
— Law Commission of India. (2009). The inclusion of victims' rights in the criminal justice system (Report No. 226).
— Lynskey, O. (2024). "Schrems III?" The future of EU–US data transfers after the Data Privacy Framework. Common Market Law Review, 61(5), 1339–1368.
— Malimath Committee. (2003). Committee on reforms of the criminal justice system. Ministry of Home Affairs.
— Ministry of Electronics and Information Technology. (2023). Digital Personal Data Protection Act, 2023.
— Ministry of Electronics and Information Technology. (2025). Digital Personal Data Protection Rules, 2025.
— Ministry of Electronics and Information Technology. (2025). Frequently asked questions on the Digital Personal Data Protection Act.
— Ministry of External Affairs. (2022). India's statements during the United Nations Ad Hoc Committee negotiations on cybercrime.
— Ministry of Home Affairs. (2023). Bharatiya Nagarik Suraksha Sanhita, 2023: Statement of Objects and Reasons.

— Ministry of Home Affairs. (2024). New criminal laws: Features and implementation. Government of India.
— M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.
— Below is Part 3 (N–S) of your APA 7th edition Reference List, alphabetically arranged, deduplicated, and formatted according to APA 7. I have retained only authoritative sources appropriate for a PhD legal research paper.
— National Forensic Sciences University. (2023). Analysis of the Bharatiya Nagarik Suraksha Sanhita, 2023: Strengthening scientific investigation. National Forensic Sciences University.
— National Legal Services Authority. (2018). Compensation Scheme for Women Victims/Survivors of Sexual Assault/Other Crimes, 2018. https://nalsa.gov.in

— NASSCOM. (2023). Industry analysis of the Digital Personal Data Protection Act, 2023. National Association of Software and Service Companies.
— Reserve Bank of India. (2018, April 6). Storage of payment system data (Circular No. DPSS.CO.OD.No.2785/06.08.005/2017-18). https://www.rbi.org.in
— Securities and Exchange Board of India. (2022). Cyber security and cyber resilience framework for market infrastructure institutions. https://www.sebi.gov.in
— Schrems v. Data Protection Commissioner (Schrems I), Case C-362/14, Court of Justice of the European Union, Judgment of 6 October 2015.
— Supreme Court of India. (2018). Witness Protection Scheme, 2018. https://main.sci.gov.in
— Svantesson, D. J. B. (2024). Data privacy management, cryptocurrencies and blockchain technology. Wolters Kluwer.
— United Nations Office on Drugs and Crime. (2013). Comprehensive study on cybercrime. United Nations. https://www.unodc.org
— United Nations Office on Drugs and Crime. (2023). Handbook on justice for victims. United Nations. https://www.unodc.org
— United Nations Office on Drugs and Crime. (2024). United Nations Convention against Cybercrime. United Nations. https://www.unodc.org
— United States Department of Commerce. (2023). EU–U.S. Data Privacy Framework Principles. International Trade Administration. https://www.dataprivacyframework.gov
— Van Ness, D. W., & Strong, K. H. (2015). Restoring justice: An introduction to restorative justice (5th ed.). Routledge.
— Voigt, P., & von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A practical guide (1st ed.). Springer.
— Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Polity Press.