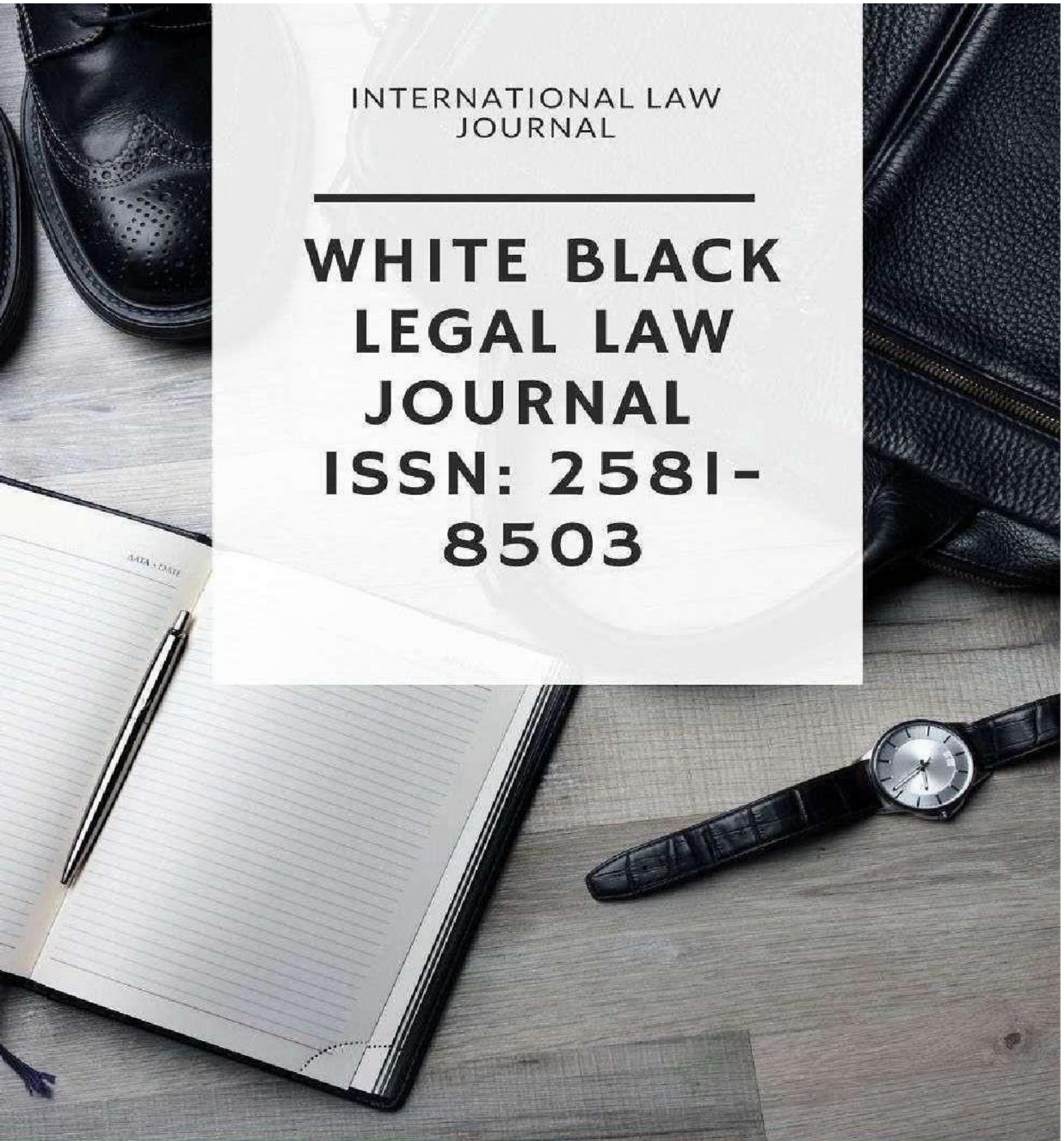




INTERNATIONAL LAW
JOURNAL

**WHITE BLACK
LEGAL LAW
JOURNAL**
**ISSN: 2581-
8503**

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

CYBER SECURITY RISK AND DATA PRIVACY IN ONLINE VIRTUAL COURT HEARINGS

AUTHORED BY - MS. SHREYA VERMA

Lecturer, Dogra Law College

Abstract

The increasing adoption of virtual court hearings has transformed the administration of justice by enabling remote access to judicial proceedings, reducing geographical barriers and supporting continuity of court functioning. However, the digitalisation of judicial processes has simultaneously created significant cybersecurity risks and data-privacy concerns. Online virtual court hearings involve the transmission and storage of highly sensitive information, including pleadings, evidence, personal data, confidential communications, audio-visual recordings and judicial documents, thereby exposing judicial institutions to risks such as unauthorised access, cyberattacks, data breaches, identity theft, interception and misuse of court records. This paper critically examines the legal and technological challenges associated with cybersecurity and data privacy in India's virtual court ecosystem. The study adopts a doctrinal and analytical legal methodology, examining the Information Technology Act, 2000, Digital Personal Data Protection Act, 2023, constitutional privacy principles under Article 21, relevant judicial decisions, procedural rules and policies governing e-Courts and virtual hearings. Particular attention is given to data minimisation, consent, confidentiality, cybersecurity safeguards, access control, data retention and institutional accountability. The study argues that although virtual courts enhance accessibility and efficiency, technological convenience cannot be permitted to compromise the confidentiality and integrity of judicial information. It recommends a comprehensive framework incorporating encryption, multi-factor authentication, secure judicial platforms, cybersecurity audits, incident-response mechanisms, judicial data-governance standards and clear accountability for data breaches. The paper concludes that sustainable virtual justice requires a balance between access to justice, technological innovation, cybersecurity and the fundamental right to privacy.

Keywords: Cybersecurity; Data Privacy; Virtual Courts; Digital Justice; Judicial Data Protection.

Introduction

The Indian judicial system has undergone substantial technological transformation through the e-Courts Mission Mode Project, particularly following the expansion of video-conferencing and virtual hearings during and after the COVID-19 pandemic. The present e-Courts Phase III (2023–2027) seeks to transform courts into digital and paperless institutions through digitisation of judicial records, e-filing, e-payments, video conferencing, cloud-based repositories and greater integration of emerging technologies.¹ As of January 31, 2026, video-conferencing facilities had been expanded across 3,240 court complexes and 1,272 jails, with more than 3.97 crore hearings conducted through video conferencing. The scale of this digital transformation demonstrates that virtual adjudication is no longer merely an emergency mechanism but an increasingly important component of India's justice-delivery system.

Virtual hearings, however, involve the collection, processing, transmission and storage of highly sensitive judicial information, including names and addresses of litigants, identification documents, pleadings, evidence, financial information, medical records, witness statements, communications between advocates and clients, and audio-visual recordings. Consequently, the digitalisation of court proceedings creates a corresponding responsibility to protect judicial information against unauthorised access, interception, manipulation, ransomware, identity theft and data breaches. The Government has acknowledged cybersecurity and data-protection concerns within the e-Courts system and has reported the use of standard security protocols, role-based access controls, secure hosting environments and cybersecurity training.²

Evolution from the Information Technology Act to the Digital Personal

Data Protection Framework

The legal framework governing cybersecurity and privacy in virtual courts has evolved significantly. The Information Technology Act, 2000 (IT Act) constituted India's foundational legislation for electronic transactions, computer-related offences and aspects of information security. Sections 43 and 43A, among other provisions, historically provided civil consequences for unauthorised access and compensation relating to failure to protect sensitive personal data by specified bodies.³ The Information Technology (Reasonable Security

¹ Department of Justice, Government of India, *e-Courts Project Phase III*, Ministry of Law and Justice, Government of India, (2023–2027), available at: [Department of Justice](#) (last visited Aug. 16, 2026).

² Press Information Bureau, Ministry of Law and Justice, Government of India, *Digitization of Courts*, Feb. 12, 2026, available at: [PIB](#) (last visited Aug. 17, 2026).

³ **Information Technology Act, 2000**, §§ 43, 43A, No. 21, Acts of Parliament, 2000 (India), available at: [India Code](#) (last visited Aug. 18, 2026).

Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 subsequently provided a regulatory framework concerning sensitive personal data and reasonable security practices.⁴ Although these provisions remain relevant to India's broader cyber-law architecture, the growth of judicial digitalisation has highlighted the need for a more comprehensive personal-data protection framework.

The Supreme Court's recognition of privacy as a fundamental right in Justice K.S. Puttaswamy (Retd.) v. Union of India marked a constitutional turning point. The nine-judge Bench held that privacy is protected as an intrinsic part of the rights guaranteed under Article 21 and other fundamental freedoms.⁵ The judgment is particularly significant for virtual courts because judicial proceedings involve information concerning individuals that may be highly personal, confidential or professionally privileged. The constitutional protection of privacy therefore requires courts and judicial institutions to balance transparency and open justice against legitimate requirements of confidentiality and data protection.

The Digital Personal Data Protection Act, 2023 (DPDP Act) represents the next major stage in India's data-protection framework. Enacted on August 11, 2023, the Act establishes a framework governing the processing of digital personal data while recognising both an individual's right to protect personal data and the need to process such data for lawful purposes.⁶ Its provisions concerning obligations of data fiduciaries, rights of data principals, security safeguards, breach-related responsibilities and penalties have direct relevance to digital judicial environments where personal data is processed on a large scale.

The legal landscape has further developed through the Digital Personal Data Protection Rules, 2025, notified on November 13, 2025. The Rules provide the implementation framework for the DPDP Act, including provisions concerning security safeguards and institutional compliance.⁷ The Government has described the 2025 Rules as establishing a practical framework for safeguarding personal data in India's expanding digital environment.⁸

⁴ Ministry of Electronics and Information Technology, Government of India, *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011*, available at: MeitY (last visited Aug. 18, 2026).

⁵ *K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1.

⁶ **Digital Personal Data Protection Act, 2023**, No. 22, Acts of Parliament, 2023 (India), available at: [India Code](#) (last visited Aug. 19, 2026).

⁷ Ministry of Electronics and Information Technology, Government of India, *Digital Personal Data Protection Rules, 2025*, G.S.R. 846(E), Nov. 13, 2025, available at: [MeitY](#) (last visited Aug. 19, 2026).

⁸ Ministry of Electronics and Information Technology, Government of India, *Explanatory Note to Digital Personal Data Protection Rules, 2025*, available at: MeitY (last visited Aug. 19, 2026).

Cybersecurity, Privacy and the Future of Digital Justice

The development of virtual courts therefore requires an integrated understanding of cybersecurity, data privacy and judicial independence. Virtual hearings create multiple points of technological vulnerability: the litigant's device, advocate's device, judicial computer systems, video-conferencing platforms, network infrastructure, cloud storage and digital case-management systems. A compromise at any stage may expose confidential judicial information or interfere with the integrity of proceedings. The risks become more significant as e-Courts Phase III expands digital repositories, artificial intelligence, OCR, interoperability and online access to judicial information.⁹

At the same time, judicial transparency remains a fundamental component of open justice. Excessive restrictions on access to proceedings could undermine public confidence and transparency, whereas unrestricted digital dissemination may expose sensitive personal information. The challenge is consequently to establish an appropriate balance between open justice and privacy protection. The Supreme Court's constitutional privacy jurisprudence provides an important framework for this balance, requiring restrictions on privacy to satisfy constitutional standards of legality, legitimate purpose and proportionality.

The present study therefore examines cybersecurity and data privacy in virtual court hearings through the combined perspectives of the IT Act, 2000, IT Rules, 2011, constitutional privacy jurisprudence, the DPDP Act, 2023, DPDP Rules, 2025 and the e-Courts framework. It argues that technological modernisation of the judiciary must be accompanied by equally sophisticated data-governance and cybersecurity mechanisms. Secure encryption, multi-factor authentication, role-based access, secure cloud infrastructure, regular cybersecurity audits, breach-response mechanisms, data minimisation, controlled recording and retention, judicial personnel training and clearly defined institutional accountability are essential for protecting the integrity of digital justice. The objective should not merely be to make courts technologically accessible, but to ensure that digital justice remains secure, confidential, constitutionally compliant and worthy of public trust.

Research objectives

1. To critically examine the cybersecurity risks associated with online virtual court hearings and assess the adequacy of India's existing legal and institutional safeguards.

⁹ Department of Justice, Government of India, *e-Courts Project Phase III*, supra note 1.

2. To evaluate the effectiveness of India's data-privacy framework in protecting personal and judicial data during virtual court proceedings and suggest appropriate legal and technological reforms.

Research methodology

The present study adopts a doctrinal and analytical legal research methodology to examine cybersecurity risks and data-privacy concerns associated with online virtual court hearings in India. The research primarily relies on secondary sources, including the Information Technology Act, 2000, Information Technology Rules, 2011, Digital Personal Data Protection Act, 2023, Digital Personal Data Protection Rules, 2025, constitutional provisions and relevant judicial decisions concerning privacy and digital rights. Government policies, e-Courts project documents, cybersecurity guidelines, reports of the Department of Justice and Ministry of Electronics and Information Technology, and authoritative institutional publications are also examined. The study analyses emerging threats including unauthorised access, cyberattacks, data breaches, interception, identity theft and misuse of judicial recordings. Judicial decisions are critically examined to understand the constitutional dimensions of privacy, confidentiality and access to justice. A comparative and critical approach is further employed to identify legislative and institutional gaps and assess whether existing safeguards adequately protect judicial and personal data. The study ultimately proposes legal, technological and institutional measures for secure and privacy-preserving virtual justice.

Analysis

1. Virtual Court Hearings and the Emergence of Cybersecurity Obligations

The first objective of the study is to critically examine the cybersecurity risks associated with online virtual court hearings and assess the adequacy of India's existing legal and institutional safeguards. The analysis demonstrates that virtual hearings have become an established component of India's justice-delivery system rather than merely an emergency response to the COVID-19 pandemic. In *In Re: Guidelines for Court Functioning Through Video Conferencing During COVID-19 Pandemic*, the Supreme Court authorised the Supreme Court and High Courts to adopt video-conferencing technologies for the continued functioning of courts and directed that facilities should be made available to litigants who lacked access to

such technology.¹⁰ The decision established the legal legitimacy of virtual adjudication while simultaneously recognising the need for procedural safeguards.

The technological basis for virtual hearings was, however, established well before the pandemic. In *State of Maharashtra v. Dr. Praful B. Desai*, the Supreme Court held that evidence could be recorded through video conferencing and interpreted the expression “presence” in a manner consistent with technological developments.¹¹ The decision is foundational because it established that technological communication could satisfy procedural requirements where the integrity of the judicial process was maintained.

The development of virtual courts nevertheless creates a new category of risk. Physical courtrooms traditionally provide a relatively controlled environment; virtual hearings distribute the proceeding across multiple devices, networks, platforms and locations. A single proceeding may involve a judge's official device, an advocate's computer, a litigant's mobile phone, a witness's device, a court server and a third-party video-conferencing infrastructure. Each point creates a potential attack surface. Risks include unauthorised entry into hearings, interception of communications, screen capture, unauthorised recording, malware, ransomware, identity impersonation, compromised credentials and disclosure of confidential documents.

The Supreme Court's **Model Rules for Video Conferencing for Courts** recognise that virtual proceedings are judicial proceedings and that ordinary judicial protocols continue to apply. The Rules also expressly prohibit unauthorised recording of proceedings.¹² This is significant because unauthorised recording can transform a confidential judicial proceeding into a permanent digital asset capable of being copied and redistributed beyond judicial control. The present e-Courts architecture has consequently moved towards stronger digital infrastructure and security. The Government has reported that video-conferencing facilities have been enabled in thousands of court complexes and that Phase III of the e-Courts Project includes substantial investment in digital infrastructure.¹³ The scale of digitisation reinforces the necessity of treating cybersecurity as an essential component of judicial administration rather than merely an information-technology concern.

¹⁰ *In Re: Guidelines for Court Functioning Through Video Conferencing During COVID-19 Pandemic*, 2020 SCC OnLine SC 355. (indiankanoon.org)

¹¹ *State of Maharashtra v. Dr. Praful B. Desai*, (2003) 4 SCC 601. (indiankanoon.org)

¹² E-Committee, Supreme Court of India, *Model Rules for Video Conferencing for Courts*, available at e-Committee, Supreme Court of India (last visited Aug. 16, 2026).

¹³ Department of Justice, Government of India, *Video Conferencing in Courts*, available at Department of Justice (last visited Aug. 17, 2026).

2. Constitutional Right to Privacy and Protection of Judicial Data

The second major finding concerns the constitutional dimension of data privacy. The Supreme Court's landmark decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India* recognised privacy as a constitutionally protected fundamental right under Article 21 and other fundamental freedoms.¹⁴ The Court described privacy as an essential aspect of human dignity and autonomy. This principle has direct application to virtual court hearings because judicial proceedings frequently involve highly sensitive personal information.

For example, family disputes may contain information concerning marital relationships, children and financial circumstances; criminal proceedings may involve medical information, addresses and witness identities; commercial litigation may reveal trade secrets and proprietary information; and sexual-offence cases may contain exceptionally sensitive personal data. Digitisation increases the possibility that such information can be copied, stored, transmitted or accessed beyond the immediate judicial purpose.

The privacy principle was further developed in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (Aadhaar), where the Supreme Court applied principles of legality, legitimate State purpose and proportionality in assessing privacy intrusions.¹⁵ The proportionality framework is particularly relevant to virtual courts because the objective of transparency and access to justice must be balanced against the need to protect personal information. Data should not be collected, retained or disseminated merely because technological systems make such collection possible.

The Supreme Court's earlier decision in *District Registrar & Collector v. Canara Bank* recognised privacy interests in relation to documents and information held by individuals and institutions.¹⁶ Similarly, in *People's Union for Civil Liberties (PUCL) v. Union of India*, the Court recognised the serious privacy implications associated with interception of communications and prescribed procedural safeguards.¹⁷ These principles acquire greater importance in virtual hearings because electronic communications may contain privileged lawyer-client communications and sensitive judicial information.

The decision in *R. Rajagopal v. State of Tamil Nadu* also recognised privacy as a significant constitutional interest, particularly concerning the publication of personal information.¹⁸ Although the case arose in the context of publication rather than virtual courts, its principle is

¹⁴ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1. (indiankanoon.org)

¹⁵ *K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 SCC 1.

¹⁶ *District Registrar & Collector, Hyderabad v. Canara Bank*, (2005) 1 SCC 496.

¹⁷ *People's Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 SCC 301.

¹⁸ *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632.

relevant to the uncontrolled dissemination of judicial information through digital platforms. Accordingly, the analysis indicates that judicial data cannot be treated merely as ordinary administrative information. It has constitutional significance, and its collection, processing, access and dissemination must be governed by principles of necessity, purpose limitation, security and proportionality.

3. Open Justice, Live Streaming and Confidentiality

Virtual hearings also create a tension between **open justice and privacy**. Transparency is an essential characteristic of judicial administration, but unrestricted digital access may create privacy risks that do not exist to the same extent in physical courtrooms. The Supreme Court addressed this tension in *Swapnil Tripathi v. Supreme Court of India*, recognising the importance of live streaming of proceedings while also emphasising the need for safeguards concerning privacy, confidentiality and sensitive proceedings.¹⁹

Following *Swapnil Tripathi*, the e-Committee formulated Model Rules for Live-Streaming and Recording of Court Proceedings. The Rules recognise privacy and confidentiality concerns involving litigants and witnesses and provide for restrictions in appropriate categories of cases.²⁰ This demonstrates that the Indian judicial system does not regard transparency as an absolute value. Instead, public access must be balanced against competing interests such as privacy, confidentiality, national security and the protection of vulnerable participants.

The Supreme Court's decision in *Santhini v. Vijaya Venkatesh* is especially relevant. The Court considered video conferencing in the context of matrimonial proceedings and observed that video conferencing can be compatible with **in-camera proceedings** where adequate privacy is maintained.²¹ The decision demonstrates that virtual technology itself is not inherently inconsistent with confidentiality. Rather, the decisive question is whether the technological environment is sufficiently controlled to prevent unauthorised access and disclosure.

The principle is particularly important for cases involving children, sexual offences, matrimonial disputes, medical information and commercial confidentiality. A virtual court platform must therefore permit courts to restrict access, control recording and protect the identity of vulnerable participants.

¹⁹ *Swapnil Tripathi v. Supreme Court of India*, (2018) 10 SCC 639. (ecommitteesci.gov.in)

²⁰ E-Committee, Supreme Court of India, *Model Rules for Live-Streaming and Recording of Court Proceedings*, available at e-Committee, Supreme Court of India (last visited Aug. 18, 2026).

²¹ *Santhini v. Vijaya Venkatesh*, (2018) 1 SCC 1. (keralacourts.in) (last visited Aug. 18, 2026).

4. Cybersecurity, Electronic Evidence and Data Integrity

The fourth finding concerns the integrity and authenticity of electronic material used in virtual hearings. Cybersecurity is not limited to preventing unauthorised access; it also involves ensuring that digital evidence has not been altered, deleted or manipulated.

In *Shreya Singhal v. Union of India*, the Supreme Court considered the constitutional implications of regulating online expression and invalidated Section 66A of the Information Technology Act, 2000 on grounds including vagueness and overbreadth.²² The decision demonstrates that cybersecurity regulation must remain consistent with constitutional freedoms. A secure digital court system cannot rely upon unrestricted governmental control over digital communication.

In *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, the Supreme Court examined the admissibility and certification of electronic evidence under Section 65B of the Indian Evidence Act, 1872.²³ The case is significant for virtual hearings because electronic records—including digital documents, recordings and other electronically generated material—must possess adequate authenticity and evidentiary reliability.

The Supreme Court's decision in *Anvar P.V. v. P.K. Basheer* similarly established the importance of compliance with statutory requirements for electronic evidence.²⁴ These decisions indicate that digitalisation of courts requires not only secure transmission but also integrity, authentication and traceability of electronic records.

The issue becomes more complicated when hearings are recorded or stored on cloud infrastructure. Any alteration to a recording, unauthorised deletion or manipulation of metadata can potentially affect the integrity of the judicial record. Consequently, courts require secure audit trails, access logs, encryption, controlled storage and mechanisms for verifying the authenticity of digital records.

5. Data Protection, Surveillance and Institutional Accountability

The emergence of the **Digital Personal Data Protection Act, 2023 (DPDP Act)** provides a new statutory context for analysing judicial data. The Act establishes obligations relating to processing of digital personal data and requires appropriate safeguards against personal-data breaches.²⁵ However, the application of data-protection obligations to judicial institutions must

²² *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

²³ *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.

²⁴ *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.

²⁵ **Digital Personal Data Protection Act, 2023**, No. 22 of 2023 (India).

be examined alongside constitutional principles, procedural law and the special requirements of judicial administration.

The Supreme Court's decision in *K.S. Puttaswamy (Retd.) v. Union of India* provides the broader constitutional framework, while *Anuradha Bhasin v. Union of India* demonstrates the Court's insistence that restrictions affecting digital communication and fundamental rights must satisfy proportionality requirements.²⁶ The judgment is relevant to virtual courts because secure digital infrastructure should not become a justification for disproportionate restrictions on access to judicial proceedings or communication.

The issue of surveillance was also considered in *Manohar Sharma v. Union of India* and, more directly in the context of alleged spyware surveillance, in *Manohar Lal Sharma v. Union of India*. In the latter case, the Supreme Court constituted an expert committee to examine allegations concerning Pegasus spyware and emphasised the importance of privacy and national security considerations.²⁷ The case reinforces the broader proposition that digital technologies can create profound risks to individual privacy when deployed without adequate safeguards.

Similarly, *Selvi v. State of Karnataka* recognised constitutional concerns surrounding involuntary techniques that interfere with personal autonomy and mental privacy.²⁸ Although the case did not concern virtual courts, its recognition of personal autonomy and privacy is relevant when considering the expanding technological capacity of judicial institutions.

Table 1. Major Judicial Decisions Relevant to Cybersecurity and Virtual Court

Hearings		
Case	Citation	Principal relevance
<i>State of Maharashtra v. Dr. Praful B. Desai</i>	(2003) 4 SCC 601	Validity of recording evidence through video conferencing
<i>R. Rajagopal v. State of T.N.</i>	(1994) 6 SCC 632	Privacy and publication of personal information
<i>PUCL v. Union of India</i>	(1997) 1 SCC 301	Privacy and interception of communications
<i>District Registrar &</i>	(2005) 1 SCC 496	Privacy in documents and

²⁶ *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.

²⁷ *Manohar Lal Sharma v. Union of India*, (2021) 5 SCC 805.

²⁸ *Selvi v. State of Karnataka*, (2010) 7 SCC 263.

<i>Collector v. Canara Bank</i>		information
<i>Selvi v. State of Karnataka</i>	(2010) 7 SCC 263	Personal autonomy and privacy
<i>Anvar P.V. v. P.K. Basheer</i>	(2014) 10 SCC 473	Electronic evidence
<i>Shreya Singhal v. Union of India</i>	(2015) 5 SCC 1	Cyber regulation and constitutional freedoms
<i>K.S. Puttaswamy v. Union of India</i>	(2017) 10 SCC 1	Fundamental right to privacy
<i>Santhini v. Vijaya Venkatesh</i>	(2018) 1 SCC 1	Video conferencing and in-camera proceedings
<i>Swapnil Tripathi v. Supreme Court of India</i>	(2018) 10 SCC 639	Live streaming and open justice
<i>K.S. Puttaswamy v. Union of India (Aadhaar)</i>	(2019) 1 SCC 1	Proportionality and informational privacy
<i>Anuradha Bhasin v. Union of India</i>	(2020) 3 SCC 637	Digital communication and proportionality
<i>Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal</i>	(2020) 7 SCC 1	Authenticity of electronic evidence
<i>Manohar Lal Sharma v. Union of India</i>	(2021) 5 SCC 805	Digital surveillance and privacy
<i>In Re: Guidelines for Court Functioning Through Video Conferencing During COVID-19 Pandemic</i>	2020 SCC OnLine SC 355	Constitutional/legal basis for virtual hearings

Source: Compiled by the researcher from Supreme Court judgments and official e-Committee materials.

The cases demonstrate that India's judicial approach to digitalisation has developed around four interconnected principles: technological facilitation of justice, protection of privacy, authenticity of electronic information and procedural fairness. The jurisprudence therefore supports virtual courts but requires appropriate safeguards against technological and privacy-related risks.

6. Critical Evaluation and Required Safeguards

The analysis establishes that India's existing legal framework provides several important safeguards, but these safeguards are distributed across different legal instruments rather than consolidated into a single judicial cybersecurity and data-governance framework. The IT Act, constitutional privacy jurisprudence, DPDP Act, e-Courts rules and judicial precedents collectively provide protection, but the rapid development of virtual hearings creates new risks requiring specialised regulation.

First, virtual court platforms should employ end-to-end encryption or equivalent high-level encryption, particularly for confidential proceedings. Second, multi-factor authentication should be mandatory for judges, court staff, advocates and other authorised participants. Third, courts should use role-based access controls so that participants receive only the information necessary for their functions. Fourth, unauthorised recording, screenshots and redistribution of proceedings should be technically restricted wherever possible and backed by appropriate legal sanctions.

Fifth, judicial institutions should establish mandatory cybersecurity audits and penetration testing of virtual-hearing infrastructure. Sixth, courts should maintain secure logs recording access, downloads, changes and other interactions with judicial data. Seventh, there should be a clearly defined incident-response mechanism for ransomware, data breaches, unauthorised access and platform compromise. Eighth, data-retention periods should be clearly defined so that recordings and personal information are not retained indefinitely without a legitimate judicial purpose.

The analysis also indicates the importance of privacy by design. Privacy should not be treated as an additional safeguard introduced after a digital system has been created. Rather, confidentiality, access control, encryption, minimisation and retention should be incorporated into the technological architecture from the beginning. This principle is particularly important for vulnerable litigants and proceedings involving children, sexual offences, matrimonial disputes, medical information and trade secrets.

Finally, the right to access justice must be preserved. The Supreme Court's video-conferencing directions expressly recognised that litigants lacking technological resources should be provided appropriate facilities.²⁹ A cybersecurity framework must therefore not create a digital divide in which only technically sophisticated litigants can effectively participate. Security and

²⁹ *In Re: Guidelines for Court Functioning Through Video Conferencing During COVID-19 Pandemic*, 2020 SCC OnLine SC 355.

accessibility must operate together.

Finding and discussion

The analysis supports the conclusion that virtual court hearings are legally valid and capable of improving access to justice, but their sustainability depends upon strong cybersecurity and privacy safeguards. The Indian judiciary has already developed substantial jurisprudence recognising video conferencing, electronic evidence, privacy, open justice and proportionality. Cases such as Praful B. Desai, Swapnil Tripathi, Santhini, Puttaswamy, Anuradha Bhasin and Arjun Panditrao Khotkar collectively demonstrate that technological innovation must remain subject to constitutional and procedural safeguards.

The existing framework should therefore not be viewed as inadequate in principle; rather, its principal weakness lies in fragmentation and implementation. The IT Act provides the foundational cyber-law framework, the DPDP Act introduces a modern data-protection regime, and the e-Courts Model Rules regulate virtual proceedings. What remains necessary is stronger integration among these frameworks through dedicated judicial cybersecurity standards, clear responsibility for data breaches, regular security audits, secure judicial cloud infrastructure and comprehensive training for judges, court staff and legal professionals.

The study consequently finds that the future of digital justice should be based upon a “secure-by-design” judicial model, in which access to justice, open justice, privacy, cybersecurity and evidentiary integrity are treated as complementary rather than competing objectives. The legitimacy of virtual courts will ultimately depend not merely on their convenience and efficiency, but on whether litigants can trust that their personal information, confidential communications and judicial records remain secure throughout the digital lifecycle.

Conclusion

The present study concludes that the emergence of virtual court hearings has significantly improved the accessibility, continuity and efficiency of judicial proceedings in India. However, the digital transformation of the justice system has simultaneously created substantial cybersecurity and data-privacy risks, including unauthorised access, interception, identity theft, data breaches, ransomware, manipulation of electronic records and unauthorised recording or dissemination of proceedings. These risks are particularly serious because court proceedings frequently contain sensitive personal, financial, medical, commercial and confidential information.

India possesses an evolving legal framework addressing these concerns through the Information Technology Act, 2000, the Information Technology Rules, 2011, constitutional privacy jurisprudence, the Digital Personal Data Protection Act, 2023, the Digital Personal Data Protection Rules, 2025, and the e-Courts and Video-Conferencing Rules. Judicial decisions such as K.S. Puttaswamy, Swapnil Tripathi, Santhini, Praful B. Desai, Anuradha Bhasin and Arjun Panditrao Khotkar demonstrate that technological innovation must remain subject to privacy, procedural fairness, evidentiary integrity and constitutional safeguards.

Nevertheless, the study finds that India's present framework remains fragmented, requiring stronger coordination and implementation. Virtual courts should adopt encryption, multi-factor authentication, role-based access controls, secure digital storage, cybersecurity audits, access logs, incident-response mechanisms and clearly defined data-retention policies. Special protection should be provided for vulnerable litigants and confidential proceedings.

Ultimately, sustainable digital justice requires a “secure-by-design” approach, balancing technological innovation with privacy, cybersecurity, transparency and access to justice. The legitimacy of virtual courts will depend upon public confidence that judicial information remains secure, confidential and constitutionally protected throughout its digital lifecycle.

Suggestions

1. Develop dedicated judicial cybersecurity standards specifically governing virtual hearings, digital evidence, recordings and judicial databases.
2. Mandate encryption and multi-factor authentication for judges, court staff, advocates and authorised participants.
3. Strengthen access controls through role-based permissions and secure identity verification.
4. Conduct periodic cybersecurity audits and penetration testing of e-Courts infrastructure and video-conferencing platforms.
5. Establish a mandatory judicial data-breach response mechanism with clearly assigned institutional responsibility.
6. Adopt privacy-by-design principles while developing and upgrading virtual court technologies.
7. Regulate recording, storage, retention and dissemination of virtual proceedings, particularly in sensitive cases.

8. Provide regular cybersecurity and data-privacy training to judges, court officials and legal professionals.
9. Strengthen protection of vulnerable litigants through restricted-access and confidential virtual hearings.
10. Ensure digital accessibility alongside cybersecurity so technological safeguards do not create barriers to access to justice.

Future scope

Future research may empirically assess cybersecurity vulnerabilities in India's virtual courts and evaluate compliance with the DPDP Act, 2023. Comparative studies could examine international judicial cybersecurity frameworks, privacy-preserving technologies, AI-enabled court systems and blockchain-based judicial records. Further research may develop measurable standards for judicial data security, breach prevention and accountability.

References

1. Department of Justice, Government of India, *e-Courts Project Phase III*, Ministry of Law and Justice, Government of India, (2023–2027), available at: [Department of Justice](#) (last visited Aug. 16, 2026).
2. Press Information Bureau, Ministry of Law and Justice, Government of India, *Digitization of Courts*, Feb. 12, 2026, available at: [PIB](#) (last visited Aug. 17, 2026).
3. **Information Technology Act, 2000**, §§ 43, 43A, No. 21, Acts of Parliament, 2000 (India), available at: [India Code](#) (last visited Aug. 18, 2026).
4. Ministry of Electronics and Information Technology, Government of India, *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011*, available at: MeitY (last visited Aug. 18, 2026).
5. **K.S. Puttaswamy (Retd.) v. Union of India**, (2017) 10 S.C.C. 1.
6. **Digital Personal Data Protection Act, 2023**, No. 22, Acts of Parliament, 2023 (India), available at: [India Code](#) (last visited Aug. 19, 2026).
7. Ministry of Electronics and Information Technology, Government of India, *Digital Personal Data Protection Rules, 2025*, G.S.R. 846(E), Nov. 13, 2025, available at: [MeitY](#) (last visited Aug. 19, 2026).

8. Ministry of Electronics and Information Technology, Government of India, *Explanatory Note to Digital Personal Data Protection Rules, 2025*, available at: MeitY (last visited Aug. 19, 2026).
9. Department of Justice, Government of India, *e-Courts Project Phase III*, supra note 1.
10. *In Re: Guidelines for Court Functioning Through Video Conferencing During COVID-19 Pandemic*, 2020 SCC OnLine SC 355. (indiankanoon.org)
11. *State of Maharashtra v. Dr. Praful B. Desai*, (2003) 4 SCC 601. (indiankanoon.org)
12. E-Committee, Supreme Court of India, *Model Rules for Video Conferencing for Courts*, available at e-Committee, Supreme Court of India (last visited Aug. 16, 2026).
13. Department of Justice, Government of India, *Video Conferencing in Courts*, available at Department of Justice (last visited Aug. 17, 2026).
14. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1. (indiankanoon.org)
15. *K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 SCC 1.
16. *District Registrar & Collector, Hyderabad v. Canara Bank*, (2005) 1 SCC 496.
17. *People's Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 SCC 301.
18. *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632.
19. *Swapnil Tripathi v. Supreme Court of India*, (2018) 10 SCC 639. (ecommitteesci.gov.in)
20. E-Committee, Supreme Court of India, *Model Rules for Live-Streaming and Recording of Court Proceedings*, available at e-Committee, Supreme Court of India (last visited Aug. 18, 2026).
21. *Santhini v. Vijaya Venkatesh*, (2018) 1 SCC 1. (keralacourts.in) (last visited Aug. 18, 2026).
22. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
23. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
24. *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
25. **Digital Personal Data Protection Act, 2023**, No. 22 of 2023 (India).
26. *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.
27. *Manohar Lal Sharma v. Union of India*, (2021) 5 SCC 805.
28. *Selvi v. State of Karnataka*, (2010) 7 SCC 263.
29. *In Re: Guidelines for Court Functioning Through Video Conferencing During COVID-19 Pandemic*, 2020 SCC OnLine SC 355.