
THE GLASS GAVEL: A COMPARATIVE STUDY OF DATA PRIVACY LAWS AND THE DOCTRINE OF PRACTICAL OBSCURITY IN THE GLOBAL EVOLUTION OF ELECTRONIC COURTS

Ms. Kshama Pandey, PhD Scholar, Presidency University, Bangalore

Prof. Dr. Saroj Sharma, Dean, School of Law, Presidency University, Bangalore

ABSTRACT

Administration of justice has been catalysed by a profound paradigm shift due to rapid transition from traditional physical courtrooms to digitized electronic courts. This transition to electronic court, not to mention virtual hearing as well has compelled to revisit few fundamental principles of law such as Open Court, Open Justice, Right to Privacy, Right to be Forgotten, Right to Erasure among others. This paper attempts to critically examine the Privacy-Transparency Dialectic emerged due to inherent tension between the mandate for judicial transparency and the right to data privacy in the digital age. The paper investigates how the Doctrine of Practical Obscurity has been dramatically eroded making digital judicial record permanent, searchable, and indexable facilitating digital stigmatization and predatory data scraping. The paper evaluates the normative legal frameworks of developed, emerging and poor jurisdictions with a particular focus on European Union General Data Protection Regulation and Indian Digital Personal Data Protection (DPDP) Act, 2023 employing comparative legal methodology.

The core argument of the paper emphasises to integrate Privacy-by-Design (PbD) including pseudonymization-by-default and de-indexing protocols so that the digitization of the judiciary, particularly judicial records shall remain a public service instead of transforming into a tool for private surveillance. The paper advocates for legislative and technical reforms for bifurcating data into public accountability data and sensitive personal data and concludes by proposing a Symmetric Transparency Model that may upholds the constitutional promise of transparency without compromising the fundamental human dignity.

I. INTRODUCTION

The global impetus towards the e-Court model characterised by electronic filing, virtual hearings, and the digitised dissemination of judgments is often lauded as a triumph of judicial efficiency and a democratisation of legal access.¹ In the traditional physical courtroom system, the open court principle, a fundamental tenets of transparent justice coexisted peacefully with individual data privacy through an unwritten structural reality, the doctrine of practical obscurity.² This doctrine was not born out of statutory text or constitutional decrees rather it was a natural byproduct of friction.³ To access court dockets, personal litigious histories, or sensitive corporate filings, an interested party had to physically travel to the court complex, search through dusty paper indexes and pay copying fees.⁴ However, adaption to the digital courtrooms has diluted the natural friction of retrieval of judicial record including personal information. By creating a glass court, where unfiltered judicial records are uploaded digitally, digital transformation of the judiciaries has dissolved the doctrine of practical obscurity making the personal misfortune permanently indexable. During traditional phase of judiciary, the ‘Open Court’ principle was mitigated by practical obscurity ensuring that even though the judicial records are legally accessible still it will not be misused due to logistical inaccessibility. E-Courts aims to make the justice delivery system transparent, affordable, accessible to all the stakeholder, and to enhance judicial productivity in terms of both quality and quantity but this shall not be attained at the cost of an individual’s right to privacy.

In *U.S. Department of Justice v. Reporters Committee for Freedom of the Press*⁵, the US Supreme Court recognised the doctrine of practical obscurity by distinguishing between decentralised paper-based records and centralised digitized government databases. The court held that an individual maintains a valid privacy interest in preventing the aggregate compilation of their public information into an easily searchable digital dossier.⁶ This paper addresses this complex intersection of open justice and right to be forgotten by undertaking a comprehensive comparative analysis of how data privacy and the doctrine of practical

¹ RICHARD SUSSKIND, *ONLINE COURTS AND THE FUTURE OF JUSTICE* (Oxford University Press 2019).

² Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 Cal. L. Rev. 1, 21-22 (2013).

³ *U.S. Dep’t of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 762-64 (1989).

⁴ Jane Kirtley, “*Misguided in Principle and Unworkable in Practice*”: *It is Time to Discard the Reporters Committee Doctrine of Practical Obscurity (And its Evil Twin, The Right to be Forgotten)*, 20 Comm. L. & Pol’y 91 (2015).

⁵ See *Reporters Comm.*, 489 U.S. at 764.

⁶ See *id.* At 771.

obscurity are maintained in different countries with primary focus on Europe and India.

This paper attempts to bridge the research gap by analysing the judiciary not merely as an adjudicatory body but as a high-volume data-processing entity that must be subject to the same rigorous data protection standards as any other public or private body.

II. CONCEPTUAL FRAMEWORK

The conceptual foundations of judicial privacy are anchored in the tension between the democratic imperative of *Open Justice* and the individual's *Right to Privacy*. Historically, this balance was maintained by the Doctrine of Practical Obscurity.⁷ In the digital epoch, this foundation is further interrogated through the theory of Contextual Integrity developed by Helen Nissenbaum.

A. The Doctrine of Practical Obscurity

According to doctrine of practical obscurity, famously articulated by the Supreme Court of the United States in the landmark case *U. S. Department of Justice v. Reporters Committees for the Freedom of the Press*⁸, judicial records remain private and effectively protected from widespread public dissemination by the physical, logistical, and financial frictions required to retrieve it. Any judicial record, even if it is classified as public record remains practically obscure as long as it is scattered, decentralised and difficult for a person to access without substantive efforts. Justice John Paul Stevens drew a sharp distinction between a piece of public data buried in an obscure local file and the centralised, electronic aggregation of that same data into a singular easily searchable digital dossier.⁹ Observing that in the digital age due to cloud storage, and automated web scraping, the doctrine of practical obscurity has collapsed to a great extent. Documents that once required a physical trip to a court complex archive are now indexed by global search engine, converting localised legal transparency into a tool for permanent social stigmatization, commercial profiling, and targeted data mining.¹⁰

⁷ HELEN NISSENBAUM, *PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE* 129 (2010).

⁸ *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 762-64 (1989).

⁹ *See id.* 751-53.

¹⁰ Daniel J. Solove, *Access and Aggregation: Public Records, Privacy, and the Constitution*, 86 Minn. L. Rev. 1137, 1139-41 (2002).

B. Open Justice V. Right To Erasure

“Publicity is the very soul of justice. It is the keenest spur to exertion, and the surest of all guards against improbity. It keeps the judges himself, while trying, under trial.”¹¹

The doctrine of Open Justice which says that justice must not only be done but must be seen to be done, is one of the fundamental principles of the common law system. In *Scott v. Scott*¹² it was established that the power of the court to sit in camera is limited to exceptional circumstances. This doctrine encompassing three verticals namely public access to hearings, access to records including inspection of documents, and freedom to report fair and accurate accounts of proceedings serves as a safeguard against judicial arbitrariness and promotes public confidence in the administration of justice. As per Article 145(4) of the Constitution of India, no judgement shall be delivered by the Supreme Court save in open court.

Today, in the era of e- courts, search engine indexing eliminates the friction of distance and the friction of time (practical obscurity). A litigant’s most sensitive personal disclosures often involving matrimonial trauma, medical history, or minor criminal lapses are permanently associated with their digital identity through name-based searches.¹³ This has challenged, an undeniable right that has been elevated to the level of fundamental rights in most of the jurisdictions, Right to Erasure (corollary to Right to be Forgotten). In *Google Spain SL v. Agencia Espanola de Proteccion de Datos*¹⁴, the Court of Justice of the European Union categorically upheld an individual’s right to be forgotten. The Court held that search engine operators are data collector and must remove links related to personal data that is inadequate, irrelevant or no longer relevant, upon request. In *Hurbain v. Belgium*¹⁵, the European Court of Human Rights Grand Chamber upholding the right of an individual involved in a car accident years ago to have the digital archives of a newspaper anonymised. In another judgement *Biancardi v Italy*¹⁶ the European Court of Human Rights ruled that de-indexing an article from a search engine was a proportionate measure to protect the reputation and privacy of an

¹¹ JEREMY BENTHAM, RATIONALE OF JUDICIAL EVIDENCE 524.

¹² *Scott v. Scott* (1913) AC 417 (HL).

¹³ Seda Gurses, Carmela Troncoso & Claudia Diaz, *Emerging Privacy by Design*, 2011 PROC. INT’L CONF. ON DATA PROT. PRIV. (2011).

¹⁴ Case C-131/12, *Google Spain SL v. Agencia Espanola de Proteccion de Datos (AEPD)*, ECLI:EU:C:2014:317 (May 13, 2014).

¹⁵ *Hurbain v. Belgium (GC)*, no. 57292/16, ECHR 2023 (Judgment 4.7.2023).

¹⁶ *Biancardi v. Italy*, No. 77419/16, ECtHR (First Section), 25 November 2021.

individual after the criminal proceedings against them have concluded.

In digital judiciary environment, the "Open Court" principle is no longer a tool for holding the state accountable rather, it has become a tool for private surveillance, creating a digital life sentence from which there is no archival escape.¹⁷

C. Contextual Integrity Theory

The application of Helen Nissenbaum's Theory of Contextual Integrity to the judicial domain provides a rigorous normative framework for understanding why the digitisation of court records feels like a violation even when the data involved is technically public. Unlike classical theories that view privacy as a binary state (private versus public), Nissenbaum posits that privacy is the preservation of informational norms within specific social contexts.¹⁸ Contextual integrity is maintained when the flow of information adheres to the entrenched norms of a given social sphere. Nissenbaum identifies four key variables that define these norms i.e. context, actors (sender, recipient, subject), attributes (type of info), and transmission principles (the "how").¹⁹ In the judicial context, these variables were clearly defined:

- Context: The Adjudicatory Sphere (seeking justice/accountability).
- Actors: Litigants (Subjects), Judges/Clerks (Recipients), and the attending public.
- Attributes: Testimony, pleadings, and personal identifiers.
- Transmission Principle: "Public accessibility" qualified by "Practical Obscurity."

When a court publishes a searchable, indexable judgment, a "Contextual Displacement" occurs. The information flows from the adjudicatory context into the commercial/general information context. While the *Attributes* (the data) remain the same, the *Recipient* and *Transmission Principles* change radically.²⁰

¹⁷ Dinasti Research, *Evaluating the Impact of Digital Judiciary on Access to Justice for Vulnerable Groups*, 2025 TECH & L. REV. 34, 42 (2025).

¹⁸ *Supra*, 127-140 (2010).

¹⁹ Philipp K. Masur et al., *Comparative Privacy Research: Literature Review, Framework, and Research Agenda*, 41 THE INFO. SOC'Y 69, 74 (2025).

²⁰ Seda Gurses, Carmela Troncoso & Claudia Diaz, *Engineering Privacy by Design*, 2011 PROC. INT'L CONF. ON DATA PROT. & PRIV. (2011).

According to this theory public data does not mean available for all purposes. Nissenbaum argues that any change in informational flow must be subjected to a "Redemptive Evaluation."²¹ If the shift to digital e-courts facilitates predatory analytics, it fails the test of contextual integrity. Therefore, a digital judiciary must implement Privacy-by-Design to restore these norms. This involves ensuring that information flows to *legal* actors for *legal* purposes while remaining obscured from *commercial* actors for *non-legal* purposes. This theoretical grounding justifies the Right to Obscurity not as an exception to transparency but as a necessary restoration of the original norms of the justice system.²²

III. THE GLOBAL LEGAL LANDSCAPE: A COMPARATIVE ANALYSIS

This comparative analysis examines the global legal landscape by categorising jurisdictions into a three-tiered typology based on their success in reconciling the Open Court principle with the Right to Privacy. At the top of this landscape lies the European Union, which has pioneered a High-Protection model. In contrast, the landscape features emerging frontiers, most notably India, where the e-Courts Mission Mode Project has achieved unparalleled scale in judicial digitisation. Finally, the analysis considers at-risk regimes jurisdictions that have aggressively digitised case files without concurrent data protection authorities, thereby leaving litigants exposed to the unregulated scraper ecosystem. This comparative enquiry is essential to identifying the research gap between technological capability and normative accountability, ultimately providing a global roadmap for a *Symmetric Transparency* model that preserves human dignity.

A. The European Union- The High Protection Model

The European Union represents the global standard in the protection of judicial privacy, underpinned by a robust fundamental rights framework. The EU's approach to e-justice is governed by the synergistic relationship between the General Data Protection Regulation (GDPR) and the Law Enforcement Directive.²³ Unlike jurisdictions that treat judicial records as absolute public property, the EU operates on the principle of Data Minimisation, asserting

²¹ HELEN NISSENBAUM, *PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE*, 182 (2010).

²² Suveer Dubey & Nandan Sharma, *A Comparative Legal Study of the GDPR and India's Digital Personal Data Protection Act*, 2026 RJ WAVE (Apr. 6, 2026).

²³ Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

that the open court mandate does not grant a perpetual license for the mass dissemination of sensitive personal metadata.²⁴

This Safe-guarder status is epitomised by the proactive implementation of Privacy-by-Design within the European e-Justice Portal. European courts increasingly adopt pseudonymisation-by-default for online judgments, ensuring that while the legal reasoning remains transparent for public accountability, the digital footprints of litigants are shielded from commercial search engine indexing.²⁵ Central to this model is the judicial application of the Right to be Forgotten which empowers individuals to prevent their past legal misfortunes from defining their digital future.²⁶

The application of the General Data Protection Regulation (GDPR) to judicial archives represents one of the most complex legal frontiers in European jurisprudence. It forces a direct confrontation between two fundamental constitutional values namely the Open Court principle, which demands transparency for democratic accountability, and the Right to Erasure (Art. 17 GDPR), which safeguards the individual's right to informational self-determination.

While the *act* of adjudication is exempt from immediate erasure to ensure the integrity of the legal record, the *dissemination* of that record on the public internet is increasingly viewed through the lens of Data Minimisation (Art. 5(1)(c)). The European Court of Justice (ECJ) and various National Data Protection Authorities (DPAs) have begun to distinguish between the archival necessity of a judgment and its online searchability.

The ECJ ruled that search engine operators are data controllers and must, upon request, remove links to personal data that are inadequate, irrelevant or no longer relevant.²⁷ Crucially, the court held that the individual's fundamental rights to privacy outweigh, as a general rule, the economic interest of the search engine and the interest of the general public in finding that information via a name-based search. In another landmark case, the ECJ held that search engine operators must de-index results that refer to legal proceedings at an earlier stage if they do not

²⁴ EUROPEAN COMMISSION, STUDY ON THE USE OF INNOVATIVE TECHNOLOGIES IN THE JUSTICE FIELD 44-50 (2020).

²⁵ Seda Gürses, Carmela Troncoso & Claudia Diaz, *Engineering Privacy by Design*, 2011 PROC. INT'L CONF. ON DATA PROT. & PRIV. (2011).

²⁶ Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*, ECLI:EU:C:2014:317 (May 13, 2014).

²⁷ *Ibid*

reflect the current position.²⁸ This case is vital for judicial archives as it mandates that digital legal history must be accurate and contemporaneous, the state cannot permit a digital life sentence based on outdated or cleared charges.

The ECJ has also clarified that while judicial authorities enjoy certain exemptions under the GDPR while acting in their judicial capacity, this immunity is not absolute. Once a judgment moves from the courtroom to a digital database for public consumption, the administrative aspect of that data processing falls under the scrutiny of the GDPR.²⁹ This distinction is critical as the *content* of the judgment is a judicial act, but its *publication* is an administrative act subject to the Right to Erasure or the Right to Pseudonymisation.

In order to resolve the conflict, European judiciaries have moved toward a model of symmetric transparency. This involves a bifurcated approach to judicial archives for example for Legal Professionals, full-text judgments with party names are maintained in secure, professional databases to ensure the development of *stare decisis* and precedential clarity and for the general public, judgments published on the open web are subject to Pseudonymisation-by-Default.³⁰

By replacing names with initials or alphanumeric codes, the EU preserves the transparency of the law while protecting the privacy of the person. This aligns with the "Privacy-by-Design" mandate (Art. 25 GDPR), where the e-justice portal is architected to prevent search engines from indexing sensitive personal metadata.³¹

The primary challenge to the Right to Erasure in judicial archives is the public interest argument. Critics argue that anonymising judgments hampers historical research and journalist scrutiny. However, the EU's Safe-guarder framework responds by asserting that the public interest in transparency is served by knowing *what* the court decided and *why*, rather than *who* was involved in a private civil dispute.³² For instance, in the Italian Supreme Court (Corte di Cassazione), a recent trend involves the "Web-Oblivion" protocol, where litigants can request the de-indexing of their names if the social utility of the information has expired. This

²⁸ Case C-136/17, *GC and Others v. Commission nationale de l'informatique et des libertés (CNIL)*, ECLI:EU:C:2019:773 (Sept. 24, 2019).

²⁹ Case C-746/18, *H.K. v. Prokuratuur*, ECLI:EU:C:2021:152 (Mar. 2, 2021).

³⁰ EUROPEAN COMMISSION, STUDY ON THE USE OF INNOVATIVE TECHNOLOGIES IN THE JUSTICE FIELD 88-102 (2020).

³¹ Seda Gürses, Carmela Troncoso & Claudia Diaz, *Engineering Privacy by Design*, 2011 PROC. INT'L CONF. ON DATA PROT. & PRIV. (2011).

³² RICHARD SUSSKIND, *ONLINE COURTS AND THE FUTURE OF JUSTICE* 62-65 (2019).

acknowledges that while the state must remember the law, the internet must be allowed to forget the individual.³³ The GDPR framework has transformed the European judiciary from a passive record-keeper into a proactive Data Fiduciary. By applying the right to erasure not as a tool for censorship, but as a mechanism for practical obscurity, the EU has successfully demonstrated that digitisation need not lead to the death of dignity. The transition from *Google Spain* to the current PbD portals represents a normative victory for the litigant, ensuring that the doors of the digital court remain open for justice, but closed for mass surveillance.³⁴

The implications for judicial archives and legal databases are twofold, creating a tension between legal history and digital stigmatisation.

- i. The Erosion of Name-Based Searches: Before *Google Spain*, a name-based search on a general engine would frequently surface a litigant's sensitive legal history as the primary result. The ruling mandates that search engines must sever the link between a person's name and outdated legal proceedings. Consequently, while a judgment remains public within a specific legal database, it is effectively removed from the global digital display window, restoring a digital version of practical obscurity.³⁵
- ii. Structural Reform of Court Portals: The decision forced legal databases to differentiate between professional legal research and casual public scrutiny. Modern European e-justice portals have responded by implementing PbD protocols. This includes the use of robots.txt directives to prevent search engines from indexing sensitive metadata and the adoption of pseudonymisation-by-default for parties in civil and family matters.³⁶
- iii. The Accuracy of Judicial Records: *Google Spain* implies a "Right to Contextual Accuracy." If a database displays an initial criminal charge but fails to index a subsequent acquittal, the "relevance" of that data is compromised. Legal databases are

³³ *AI and Digital Justice in EU Labor Law: A Comparative Study on Predictive Tools and Judicial Transformation*, PMC (Jan. 29, 2026), <https://pmc.ncbi.nlm.nih.gov/articles/PMC12894374/>.

³⁴ Dinasti Research, *Evaluating the Impact of Digital Judiciary on Access to Justice for Vulnerable Groups*, 2025 TECH & L. REV. 34, 45-50 (2025).

³⁵ HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 129 (2010).

³⁶ EUROPEAN COMMISSION, STUDY ON THE USE OF INNOVATIVE TECHNOLOGIES IN THE JUSTICE FIELD 88 (2020).

now under a heightened fiduciary duty to ensure that digital legal records are contemporaneous and reflective of the final judicial outcome.³⁷

In conclusion, *Google Spain* ensures that the "Open Court" principle is not a license for the permanent digital shaming of litigants. It affirms that while the state must remember the law, the internet must be permitted to forget the individual.³⁸ Consequently, the EU model serves as the primary normative benchmark for *Symmetric Transparency*, demonstrating that a modern judiciary can be both technologically advanced and human-rights compliant.³⁹

B. INDIA: The Evolving Frontier

India, the largest democracy in the world, also having the most powerful apex court represents the world's most daunting high velocity transformation from archaic, paper dependent traditional judiciary to an advanced data-driven e-court ecosystem. However, developed countries across the world are discussing about integration of artificial intelligence to judgement making, India is yet to provide an adequate normative framework and infrastructure for virtual hearing and online proceedings. Realising and recognising the unmatched potential the technology has to contribute in good governance, the Government of India introduced National e- Governance Plan (hereinafter NeGP) in the year 2006. The NeGP consists of 31 Mission Mode Projects responsible to promote e-Governance. With the objective of modernising and revamping Indian traditional courts, e- Court Mission Mode Project was inaugurated. The nodal governing body for e- Court Mission Mode project is e- Committee, Supreme Court of India established in the year 2006 with the task of supervising the e- Court projects idealised under the National Policy and Action Plan for implementation of Information and Communication technology- 2005. The project is a pan India project spearheaded by Department of Justice, Ministry of Law and Justice, Government of India. The e-judiciary vision involves efficient and time bound citizen centric services, automatic procedure to provide transparency, enhancing qualitative and quantitative judicial productivity as mentioned in e- Courts Project Litigant's Charter.

E- court Mission Mode Project is a pan India project committed to deliver the promise of e-

³⁷ Suveer Dubey & Nandan Sharma, *A Comparative Legal Study of the GDPR and India's Digital Personal Data Protection Act*, 2026 RJ WAVE (Apr. 6, 2026).

³⁸ RICHARD SUSSKIND, *ONLINE COURTS AND THE FUTURE OF JUSTICE* 62 (2019).

³⁹ *AI and Digital Justice in EU Labor Law: A Comparative Study on Predictive Tools and Judicial Transformation*, PMC (Jan. 29, 2026), <https://pmc.ncbi.nlm.nih.gov/articles/PMC12894374/>.

Judiciary. The project is divided into three phases: With practical and foundational approach, Phase I focused on creating the basic digital backbone for the future e- Judiciary. This phase targeted on capacity building i.e. preparing court infrastructure, computerization of district and taluka courts, digitization of records, enabling necessary tools to equip judges to function in a technology driven environment. Phase II essentially focuses on widespread automation and Phase III aiming for a transformative push towards accessible, economical, paperless and inclusive courts.

India's status as an evolving frontier is defined by its complex Privacy-Transparency dialectic. The Supreme Court of India in the landmark *Justice K. S. Puttaswamy v. Union of India*⁴⁰ case elevated the right to privacy to a fundamental constitutional guarantee however the practical implementation of this right within the digital judicial infrastructures remains in flux. Even though the Digital Personal Data Protection (DPDP) Act, 2023 introduces a formal regulatory framework yet it contains significant carve-outs for the judicial functions and the enforcement of legal rights creating a precarious landscape for litigant data. Unlike the European Union's Safeguarder model, the Indian frontier is currently grappling with the unintended consequences of frictionless transparency where the mass availability of unredacted judgements has facilitated an unregulated market for predatory data analytics.⁴¹ Consequently, India stands at a critical juncture with the task of architecting a 'Privacy-by-Design' framework that fulfils the Puttaswamy mandate without compromising the monumental gains made in judicial efficiency.⁴²

C. JURISDICTIONS AT RISK

Legal systems primarily in the Global South or rapidly developing economies that have aggressively pursued judicial digitisation as a panacea for inefficiency without concurrently establishing robust data protection frameworks or "Privacy-by-Design" (PbD) protocols are considered as jurisdiction at risk. The Open Court principle, in these jurisdictions, is technologically hyper-charged, transforming judicial transparency from a tool of democratic accountability into a mechanism for uncontrolled surveillance.

⁴⁰ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

⁴¹ Suveer Dubey & Nandan Sharma, *A Comparative Legal Study of the GDPR and India's Digital Personal Data Protection Act*, 2026 RJ WAVE (Apr. 6, 2026).

⁴² Dinasti Research, *Evaluating the Impact of Digital Judiciary on Access to Justice for Vulnerable Groups*, 2025 TECH &L. REV. 34 (2025).

Governments prioritise the e-court such as electronic filing, virtual hearings, and public-facing judgment portals because these provide immediate, visible metrics of judicial progress. However, data encryption, access controls, and de-indexing protocols is frequently neglected.⁴³ In many at-risk jurisdictions, judicial records are published as searchable PDFs or HTML pages that are intentionally made discoverable to enhance the court's visibility. While this serves the goal of transparency, it ignores the frictionless transmission problem. Unlike the European Safe-guarder model, where the judiciary acts as a Data Fiduciary, at-risk jurisdictions often treat judicial data as abandoned once it is uploaded, allowing any third-party entity to scrape, store, and monetise it without oversight.⁴⁴

The most immediate consequence for at-risk jurisdictions is the emergence of a predatory scraper ecosystem. In the absence of legislative barriers like the GDPR's "Right to Erasure" or technical barriers like robots.txt exclusion, private legal-tech firms and background-check startups harvest millions of un-redacted records.⁴⁵ These firms create shadow databases that persist even if a court later decides to seal a record or an individual is acquitted. For a litigant in an at-risk jurisdiction, this creates a Digital Life Sentence.

Many at-risk jurisdictions are attempting to leapfrog traditional judicial development by integrating Artificial Intelligence (AI) and Predictive Analytics into their e-court frameworks. While AI can assist in clearing backlogs, its deployment in a privacy vacuum is hazardous. If predictive models are trained on un-redacted, biased, or outdated judicial data, they may institutionalise discrimination against certain demographics.⁴⁶

Furthermore, the lack of contextual integrity in these regimes means that data collected for a specific legal purpose (e.g., a bail application) is often re-purposed for state surveillance or social credit style monitoring. In these contexts, the "Open Court" principle is subverted; it no longer holds the judge accountable to the public, but instead holds the private citizen accountable to the state's digital gaze in perpetuity.⁴⁷

⁴³ RICHARD SUSSKIND, ONLINE COURTS AND THE FUTURE OF JUSTICE 145-150 (2019).

⁴⁴ HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 129 (2010).

⁴⁵ *Ibid.*

⁴⁶ *AI and Digital Justice in EU Labor Law: A Comparative Study on Predictive Tools and Judicial Transformation*, PMC (Jan. 29, 2026), <https://pmc.ncbi.nlm.nih.gov/articles/PMC12894374/>.

⁴⁷ Philipp K. Masur et al., *Comparative Privacy Research: Literature Review, Framework, and Research Agenda*, 41 THE INFO. SOC'Y 69, 75 (2025).

IV. FINDINGS AND NORMATIVE PROPOSALS

The synthesis of comparative data between jurisdictions like European Union and India provides a compelling empirical basis for the hypothesis that Privacy-by-Design (PbD) is not merely a technical requirement, but a fundamental pillar of public trust in the digital judiciary. The public willingness to engage with e-courts depends less on the speed of the internet and more on the state's ability to function as a data fiduciary.

Comparative evidence from jurisdictions lacking PbD shows a rising privacy paradox. In these regions, while the speed of case disposal may increase due to digitisation, public anxiety regarding digital recidivism also escalates. Data from at-risk Jurisdictions indicates that vulnerable groups specifically those in matrimonial and labour disputes often hesitate to seek legal redress because they fear the permanent "digital footprint" created by un-redacted judgments.⁴⁸ The Open Court principle is perceived more as a threat rather than a safeguard as a person's life is indexed by global search engines, the judiciary loses its character as a sanctuary of justice. The lack of technical barriers like robots.txt enforcement creates a trust deficit, as litigants feel the state has "abandoned" their data to the predatory scraper ecosystem.⁴⁹

Further, data from the European e-Justice portal suggests that the integration of PbD directly correlates with higher levels of institutional trust. By ensuring that legal reasoning is public while personal metadata is protected, the EU model achieves symmetric transparency.

Comparative studies show that litigants in PbD-compliant systems are more likely to participate in mediation and open-court proceedings because they are assured that their "past legal misfortunes" will not define their digital future.⁵⁰ Also, the implementation of *Tiered Access Models* prevents mass-harvesting by background-screening firms. Evidence suggests that when the state actively blocks "scraper bots," it reinforces the perception of the judiciary as a protector of human dignity.⁵¹

⁴⁸ Suveer Dubey & Nandan Sharma, *A Comparative Legal Study of the GDPR and India's Digital Personal Data Protection Act*, 2026 RJ WAVE (Apr. 6, 2026).

⁴⁹ HELEN NISSENBAUM, *PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE* 147 (2010).

⁵⁰ EUROPEAN COMMISSION, *STUDY ON THE USE OF INNOVATIVE TECHNOLOGIES IN THE JUSTICE FIELD* 102 (2020).

⁵¹ Seda Gürses, Carmela Troncoso & Claudia Diaz, *Engineering Privacy by Design*, 2011 PROC. INT'L CONF. ON DATA PROT. & PRIV. (2011).

In India, the transition toward Phase III of the e-Courts Project is a direct response to the Puttaswamy Mandate, which highlighted that privacy is a prerequisite for the exercise of all other fundamental rights. Synthesis of recent pilot projects in India indicates that when courts proactively pseudonymise names in sensitive cases (such as those involving sexual offences or minors), the "legitimacy" of the digital record is enhanced.⁵²

Suggestions for the Supreme Court of India and the European e-Justice Portal

The following policy roadmap outlines strategic interventions for the Supreme Court of India and the European e-Justice Portal to bridge the "Technical Gap" and solidify their roles as global safe-guarders of judicial privacy.

I. Suggestions for the Supreme Court of India to align with the *Puttaswamy* mandate:

- **Codification of "Judicial Data Fiduciary" Standards:** The Supreme Court should issue administrative guidelines explicitly defining the judiciary's role as a Data Fiduciary. This would mandate that the National Judicial Data Grid (NJDG) adopts Pseudonymisation-by-Default for all trial-court records, ensuring that litigants in matrimonial, labor, and minor criminal matters are shielded from general search engine indexing.⁵³
- **Mandatory Technical Barriers:** The e-Committee must enforce the implementation of robots.txt directives and advanced CAPTCHA protocols across all District and High Court portals. This would effectively disable the "frictionless" scraping of metadata by predatory analytics firms, restoring a digital version of Practical Obscurity.⁵⁴
- **AI-Driven Redaction Clearinghouse:** Establish a centralized, AI-driven redaction unit that utilizes Natural Language Processing (NLP) to scrub personal identifiers from judgments before they are uploaded to the public NJDG.

II. While the EU serves as a global benchmark, the rise of "Shadow Databases" requires a more

⁵² E-COMMITTEE, SUPREME COURT OF INDIA, DIGITAL COURTS VISION & STRATEGY (PHASE III) 18 (2023).

⁵³ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

⁵⁴ E-COMMITTEE, SUPREME COURT OF INDIA, DIGITAL COURTS VISION & STRATEGY (PHASE III) 18 (2023).

aggressive technical and cross-border stance. Suggestions for the European e-Justice Portal:

- Unified Pseudonymisation Protocols: The European e-Justice Portal should move beyond mere recommendations and implement a unified, cross-border pseudonymisation standard. This ensures that a litigant's data is protected equally whether their case is heard in Estonia or Italy, preventing "privacy arbitrage" within the Union.⁵⁵
- The "Right to be Forgotten" API: The EU should develop a specialized API for search engines and legal-tech scrapers. This API would provide real-time updates on "erasure orders" and "anonymization requests," legally compelling third-party databases to synchronize their archives with the court's official redacted record.⁵⁶
- Regulation of Predatory Analytics: In coordination with National DPAs, the EU must classify "judicial data scraping for commercial risk-scoring" as a high-risk activity under the AI Act. This would restrict the use of court data in automated credit and employment vetting unless explicit, high-level safeguards are met.⁵⁷

V. CONCLUSION

The transition from paper-based archives to high-velocity e-court ecosystems represents the most significant shift in the administration of justice since the move from oral tradition to written record. However, the rush toward judicial digitisation has occurred within a normative vacuum, one where the "Open Court" principle has been technologically hyper-charged while the individual's right to dignity and right to privacy has been systematically neglected. In these final reflections, the core arguments for a "Privacy-by-Design" (PbD) judiciary and issue a call to action for a global legal architecture that treats the state as a fiduciary of digital identity are reaffirmed.

The central argument of this research is that the state's role in the digital judiciary must evolve from a passive record-keeper to an active data fiduciary. The evidence from our comparative analysis of the European "Safeguarder" model and India's "Evolving Frontier" reveals that digitisation is not a neutral act. The 'Scraper Ecosystem' could weaponize an un-redacted

⁵⁵ Regulation 2016/679 (General Data Protection Regulation), 2016 O.J. (L 119) 1, art. 25.

⁵⁶ Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*, ECLI:EU:C:2014:317 (May 13, 2014).

⁵⁷ *AI and Digital Justice in EU Labor Law: A Comparative Study on Predictive Tools and Judicial Transformation*, PMC (Jan. 29, 2026), <https://pmc.ncbi.nlm.nih.gov/articles/PMC12894374/>.

judgement uploaded to the NJDG or European e-justice portal hence e-judiciary is not merely fulfilling a transparency mandate but also creating a permanent digital asset that may be jeopardised. In *Justice K. S. Puttaswamy v. Union of India*⁵⁸ a new judicial duty of care was recognised, this constitutional duty requires the state to recognise that informational self-determination is a prerequisite for access to justice likewise in Europe, GDPR framework provides the statutory basis for the abovementioned duty. The 'State as a Protector of Digital Dignity' is not a secondary policy goal but a foundational requirement for the legitimacy of any digital rule of law.⁵⁹ Judicial transparency must be granular. While researchers and professionals require full-text access for the development of *stare decisis*, the casual digital observer should only see pseudonymised data.⁶⁰

The "Open Court" is meant to hold the judge accountable to the public, not the private citizen accountable to the scraper. By restoring this balance, we ensure that the judiciary remains a sanctuary where individuals can seek justice without the fear of a lifelong digital stigma.⁶¹

As we conclude this analysis, we issue a clear call to action for judicial administrators, legislators, and the legal-tech community. Every e-court portal must be architected with technical barriers including robots.txt enforcement, CAPTCHAs, and AI-driven pseudonymisation as its baseline setting. Privacy cannot be a "request" made by the litigant; it must be a "gift" provided by the system.⁶² Legislatures must move beyond the "Right to be Forgotten" (which is reactive) and recognize a proactive Right to Obscurity. This right should ensure that trial-level records are shielded from commercial search engine indexing, protecting the "fresh start" that is essential for social rehabilitation.⁶³ The unregulated harvesting of judicial data for commercial risk-scoring must be recognized as a high-risk activity. Judiciaries must implement data usage agreements that legally bind third-party scrapers to respect redactions and de-indexing orders in real-time.⁶⁴ The doors of the digital court must remain open, but they must no longer lead to a digital panopticon.

⁵⁸ *Justice K. S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

⁵⁹ Suveer Dubey & Nandan Sharma, *A Comparative Legal Study of the GDPR and India's Digital Personal Data Protection Act*, 2026 RJ WAVE (Apr. 6, 2026).

⁶⁰ RICHARD SUSSKIND, *ONLINE COURTS AND THE FUTURE OF JUSTICE* 62 (2019).

⁶¹ HELEN NISSENBAUM, *PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE* 129 (2010).

⁶² ANN CAVOUKIAN, *PRIVACY BY DESIGN: THE 7 FOUNDATIONAL PRINCIPLES* (2009).

⁶³ Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*, ECLI:EU:C:2014:317 (May 13, 2014).

⁶⁴ E-COMMITTEE, SUPREME COURT OF INDIA, *DIGITAL COURTS VISION & STRATEGY (PHASE III)* 18 (2023).

BIBLIOGRAPHY:

I. Primary Sources

A. Statutes and Regulations

- Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
- Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.
- Directive (EU) 2016/680, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences, 2016 O.J. (L 119) 89.

B. Cases

- Google Spain SL v. Agencia Española de Protección de Datos (AEPD), Case C-131/12, ECLI:EU:C:2014:317 (May 13, 2014).
- GC and Others v. Commission nationale de l'informatique et des libertés (CNIL), Case C-136/17, ECLI:EU:C:2019:773 (Sept. 24, 2019).
- H.K. v. Prokuratuur, Case C-746/18, ECLI:EU:C:2021:152 (Mar. 2, 2021).
- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

II. Secondary Sources

A. Books

- ANN CAVOUKIAN, PRIVACY BY DESIGN: THE 7 FOUNDATIONAL PRINCIPLES (Information and Privacy Commissioner of Ontario, 2009).
- HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY,

AND THE INTEGRITY OF SOCIAL LIFE (Stanford University Press, 2010).

- RICHARD SUSSKIND, ONLINE COURTS AND THE FUTURE OF JUSTICE (Oxford University Press, 2019).

B. Journal Articles & Academic Papers

- Seda Gürses, Carmela Troncoso & Claudia Diaz, *Engineering Privacy by Design*, 2011 PROC. INT'L CONF. ON DATA PROT. & PRIV. (2011).
- Philipp K. Masur et al., *Comparative Privacy Research: Literature Review, Framework, and Research Agenda*, 41 THE INFO. SOC'Y 69 (2025).
- Suveer Dubey & Nandan Sharma, *A Comparative Legal Study of the GDPR and India's Digital Personal Data Protection Act*, 2026 RJ WAVE (Apr. 6, 2026).
- Dinasti Research, *Evaluating the Impact of Digital Judiciary on Access to Justice for Vulnerable Groups*, 2025 TECH & L. REV. 34 (2025).
- AI and Digital Justice in EU Labor Law: A Comparative Study on Predictive Tools and Judicial Transformation, PMC (Jan. 29, 2026), <https://pmc.ncbi.nlm.nih.gov/articles/PMC12894374/>.

C. Reports and Government Documents

- E-COMMITTEE, SUPREME COURT OF INDIA, DIGITAL COURTS VISION & STRATEGY (PHASE III) (2023).
- EUROPEAN COMMISSION, STUDY ON THE USE OF INNOVATIVE TECHNOLOGIES IN THE JUSTICE FIELD (Final Report, 2020).
- EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA), PRIVACY BY DESIGN IN DATA PROTECTION: CONCEPTS AND OPERATIONALISATION (2019).