

The Right to be Forgotten v. The Public Record: Information Privacy of the Accused in Adversarial and Inquisitorial Systems

Charitha R. Reddy¹

Abstract

The digitalisation of judicial records has significantly disrupted the equilibrium between public access to information and individual privacy, thereby triggering a major constitutional conflict in the criminal justice system. In present-day democracies, a person's digital footprint managed by the state largely determines their ability to re-enter the society. This paper presents a comparative analysis of how different legal systems tackles the issue of informational privacy, open justice and the newly recognized Right to be Forgotten.

Inquisitorial systems, which mainly operate under the European civil law, emphasize the accused's dignity and right to rehabilitation. Therefore, European legislation, spearheaded by the General Data Protection Regulation (GDPR) and the landmark Google Spain judgement, is gradually restricting public access to criminal records and even regard the removal of digital records as a rational consequence of the sentence completion. In contrast, adversarial systems, such as the United States of America, the United Kingdom, and India, are historically based on the common law principle of open justice. These countries regard court documents as permanent public property, essential for democratic transparency and institutional accountability.

But the unchecked release of criminal records online acts as an everlasting digital watchtower, subjecting the accused to unending, extra-judicial punishment, and at the same time, it weakens the restorative aspects of justice. While highlighting the strict control of information in civil law systems and contrasting it with the evolving privacy jurisprudence in common law courts such as India's post -Puttaswamy framework, this paper puts forward the position that traditional

adversarial, absolute openness is becoming less and less consistent with human rights in this era of information. The paper concludes that adversarial democracies must incorporate inquisitorial data safeguards so as not to allow publicly available information to be tool of permanent social exile.

Keywords: Right to be Forgotten, Informational Privacy, Adversarial System, Open Justice, Digital Panopticon

Introduction

The architecture of human memory is fundamentally designed to forget. In fact, this natural loss of information has historically played an essential role in social functioning through the criminal justice system by letting the past offenses of the persons be forgotten and socially reintegrated in the community. But the computerization of court records has completely changed this biological truth and created a system of perfect and forever memory (Mayer-Schönberger, 2009). The internet functions as a 'digital panopticon' -- a realm where criminal accusations, court hearings, and convictions are recorded, indexed, and made available worldwide at any time. As a result, the digital world has caused a major constitutional conflict between two opposing democratic values: the right of the public to have access to judicial information (Open Justice) and the right of an individual to be reintegrated into society (Rehabilitation and Informational Privacy).

To understand this tension, it is essential to first breakdown the assumption that complete transparency always leads to the public good. In fact, it is quite the opposite as Solove (2003) articulates "the virtues of knowing less," arguing that although information sharing enables a democracy to hold its leaders accountable,

¹Student, LL.M. (Commercial Law), CMR University, School of Legal Studies, Bengaluru.

empowering individuals through unlimited exposure of one's history may drastically curtail their future autonomy. For instance, an individual becomes subject to a practically perpetual, extra-judicial punishment as one can obtain through a search engine, court documents like acquittals, dismissals, or completed sentences. The stigma of having a digital record works independently of the formal justice system and thus it actually hinders people from finding employment, getting housing, and even socializing even after their legal obligations have been fulfilled (Jacobs, 2015).

It is this very fact that equally thwarts the system's aim to reform offenders. Rehabilitation, if based on the idea that a person can change and be reintegrated into society as a law-abiding member, then the concept of an "infinite criminal record" compels the destruction of this very hope (Jacobs, 2015). The person's entire identity is now confined to the most infamous moment of their life, so to speak, preserved as a digital amber that prevents their sociological growth.

In fact, the manner in which democracies manage this tension is a reflection of their foundational legal paradigms. This paper will explore the conflict between information privacy and open justice in the judicial process is met in a completely different way across various countries. Primarily, European civil law-based inquisitorial systems, structurally grant a high level of importance to the honour and privacy of the defendant. They consider the deletion of digital footprints as a manifestation of the criminal's reformation. On the other hand, adversarial setups such as those of the US, UK, and India are fundamentally, based on the common law doctrine of open justice. Thus, they regard judicial documents as indefinitely accessible public assets, which play a vital role in ensuring transparency of the judiciary and preventing any form of judicial tyranny.

By juxtaposing the rigid informational control of civil law regimes against the evolving privacy law in common law courts, this paper seeks to assess if the long-standing adversarial dependence on total open justice still aligns with basic human rights in this era of information. In fact, it hypothesizes that if adversarial democracies do not adopt a set of data-masking protective measures- like the

emerging "Right to be Forgotten" -- then, the public record will not be a means through which accountability is ensured but rather, an instrument of permanent social exile.

The Inquisitorial Paradigm: Dignity and the Right to Forgive

Inquisitorial legal systems, which are widespread in continental Europe, view the relationship between criminal justice and public information from a radically different philosophical standpoint than their common law counterparts. Whiteman (2004) famously noted that European privacy law mainly concerns with the protection of a person's dignity and honour, which is a complete departure from the US model focused on individual liberty against state interference. In adversarial systems, the citizens' rights to watch over the government are paramount whereas in European civil law, human dignity is safeguarded through constitutional provisions. While adversarial systems allocate the public's right to examine state actions as the paramount, European civil law, on the other hand, prioritizes the constitutional protection of human dignity. In this perspective, the criminal justice system is not seen as a public spectacle for general consumption; rather, it is essentially a state-controlled rehabilitation tool. Hence, once a convicted person has served their sentence, in most cases, their criminal record is a confidential state document rather than a public one. The state takes a paternal role in protecting the reformed individual from the social disapproval associated with the past and ensuring that the previous wrongdoings do not forever deprive the individual of future freedom.

Conversely, the borderless architecture of the internet fundamentally changed this model centred on the dignity of a person. Global search engines started to gather and show old news pieces, judicial decisions and crime records; thereby not only circumventing domestic civil law shelter but also exposing European people to a scattered, everlasting criminal record. To reestablish the equilibrium between digital memory and human dignity, the Court of Justice of the European Union (CJEU) issued its profound judgement in *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD)* (2014).

In this seminal judgement, the CJEU decided that search engines are data controllers therefore they are obliged to adhere to EU data protection directives. More crucially, the Court acknowledged that people have the right to request the removal of links to information that is inadequate, irrelevant or no longer relevant to the original purposes of its processing, the initial publication being exactly legal and accurate. The Google Spain ruling effectively birthed the modern "Right to be Forgotten", serving as a digital defence of the rehabilitative deal.

By empowering individuals to sever the digital links between their names and their past mistakes, the CJEU acknowledged that continuous public availability of one's prior criminal records in the digital world causes a disproportionate interference in a person's fundamental right to privacy. This is essentially underlining the fact that society has a corresponding 'right to forgive' (Rustad & kulevska, 2015). Most importantly, this provision does not require the removal of the original news article or court record from the source website and this way the historical and journalistic archives are preserved. What happens is that the individual is no longer searchable through his or her ex-post information, which is the source of digital panopticon, and this makes him or her able to regain control over the digital narrative.

Later on, this judicial change was also incorporated and enhanced to some extent in Article 17 of the GDPR, which officially recognised the 'Right to Erasure.' According to the GDPR, data controllers are required to delete personal information without delay when such data is no longer necessary for the original purposes of the collection, or when the continued processing of data is harmful to the public interest. Although Article 17 provides some exceptions for the right to freedom of expression and information, the overall presumption in the European framework is strongly protective of the data subject's dignity.

Ultimately, by advocating for data protection legislation as a logical accompaniment to criminal rehabilitation, the inquisitorial system actively breaks down the digital panopticon. It legally mandates a form of digital amnesia to serve a

higher sociological good. Nevertheless, though this system is great at safeguarding individual dignity, it still, to a large extent, hands over the thorny constitutional balancing acts such as balancing transparency with privacy rights to the discretion of private technology companies.

The Adversarial Tradition: Open Justice and the Eternal Record

In sharp contrast, the inquisitorial systems with their dignity-centric model focus on the dignity of the individual as the core principle of justice. On the otherwise, the adversarial jurisdictions which are based on the Anglo-American common law tradition derive their main principle of justice from the idea of open courts. According to this view, making things public is not merely an administrative preference; it is actually the basis of democratic power. The idea behind this point of view was clearly set forth by Jeremy Bentham who holds that justice can only be done in public and that by doing so judges are kept accountable and citizens are protected from the secret tribunals that are typical of authoritarian regimes. But quite a few authors point out that this complete faith in open justice may turn into a perpetuated way of public shaming especially when brought into the digital environment (Townend, 2017). So, in addition to court hearings and judgments, even criminal histories have been regarded as public property under the adversarial system. In this legal system the right to be informed of and to be present at the trial is viewed as more important than the defendant's right to privacy of personal information.

This strict adherence to transparency principle however led to some disastrous social implications of the digital era. In this seminal work, *The Eternal Criminal Record*, Jacobs (2015) dissects how the American criminal justice system uses (weaponizes) historical data. Although most of the European systems do not disclose criminal records of the persons who have been rehabilitated, in the United States, the criminal history is used in a very large scale. According to Jacobs, online availability of arrest records, photographs, and jail sentences has led to the development of a permanent digital underclass. Companies that check backgrounds, data brokers, and public

registries collect court data to identify risky individuals, thus changing the criminal sentence responsibility from the government to the private sector. To a large extent, it is the nature of the adversarial system which anticipates the perpetual risk anticipates the perpetual risk management notion rather than the reintegration of the offender. Jacobs (2015) asserts that the digital panopticon ensures that the criminal record is never entirely erased; it only goes unrecognized until the search algorithms bring it back to the public awareness, thus constantly undermining the idea of rehabilitation (Jacobs, 2015).

The strong First Amendment protection culture of the United States mainly shields its digital public sphere from being subject to European-style data erasure. On the other hand, the UK is at quite a conflicted point of the spectrum. As a common law jurisdiction deeply tethered to open justice, yet historically bound by the European human rights framework (before and during the Brexit transition), the UK has been forced to legally adjudicate on the direct clash between adversarial transparency and the Right to be Forgotten.

It was this constitutional discord that caused the High Court to give the landmark decision in *NT 1 & NT 2 v. Google LLC* (2018). The issue was involving two businessmen, who were convicted of different crimes several years ago, were released, and whose convictions were legally "spent" as per the UK's Rehabilitation of Offenders Act 1974 (hereinafter RO Act, 1974). Both individuals requested the court to order Google to delete the links to their former criminal records from search results, claiming that the continued online publication of these records infringed their privacy and hindered their rehabilitation efforts.

Justice Warby's ruling in this matter vividly portrays the legal battle to a balance between these competing rights. The Court performed a delicate and complete balancing exercise, during which it took into account, on one side, the claimant's right to privacy under Article 8 of the European Convention on Human Rights and, on the other, the public's right to freedom of expression and information under Article 10. Interestingly, the Court reached a different outcome for each claimant. NT1's claim was rejected; the Court

believed that the proofs demonstrated that he had not show remorse, that he was still a member of a public-facing company, and that the public continued to have a legitimate interest in being informed of his past financial dishonesty. On the other hand, NT2 succeeded. The Court mandated Google to delink his records, highlighting his sincere rehabilitation, the fact that he was younger at the time of the offense, and also that there was no compelling public interest in his specific historical crime (*NT 1 & NT 2 v. Google LLC*, 2018).

The judgment of *NT 1 & NT 2* highlights the depth of reluctance in common law courts to mandate digital amnesia. In contrast to the inquisitorial system that features a built-in presumption for erasure after sentencing, the adversarial system considers erasure to be a very rare remedy which has to be justified in detail, because the main rule is open justice. The UK method shows that, although adversarial systems acknowledge that the digital panopticon can be extremely harmful, they are not prepared to give up the public record completely and so they hold that the "right to know" can only be taken away when historical data is no longer of any public use.

The Indian Jurisprudential Shift

India occupies a delicate position in this global division of jurisprudence. India inherited the British legal adversarial tradition and it zealously guards the court openness principle. The Hon. Supreme Court has, time and again, held that providing the public with access to Judiciary is the fundamental right under Article 19(1)(a) of the Constitution. Access to courts is a democratic necessity aimed at ensuring the accountability of the judiciary through the public availability of judgements for decades.

The Supreme Court of India has, time and again, maintained that granting public access to judicial proceedings is the very essence of giving the fundamental right to freedom of speech and expression under Article 19(1)(a) of the Constitution. Access to courts was not just a mere procedural default but a democratic necessity aimed at ensuring the accountability of the judiciary for the public availability of

judgments for decades. However, the emergence of digital legal repositories, most notably such platforms as Indian Kanoon, have unintentionally turned India into a digital panopticon. Unredacted judgments disclosing acquittals, quashed FIRs, and family disputes were indexed globally by search engines, exposing people and continuously digital stigmatizing them even after their formal exoneration.

There was a significant change in the constitutional paradigm when the SC in a 9-judge bench decision delivered a historic judgment in the case of *Justice K. S. Puttaswamy (Retd.) v. Union of India* (2017). The Court in its unanimous verdict upheld the Right to Privacy as an essential component of the Right to Life and Personal Liberty under Article 21. What is interesting is that Justice Sanjay Kishan Kaul in his separate but concurring judgement brought the European right to be forgotten directly into Indian constitutional law. He recognised the permanence of the digital age and that people's right to protect their good name from being always linked to their past mistakes is upheld by the right to privacy. Along these lines, he also remarked that the right to privacy includes the right to one's digital life. On the other hand, similar to the hesitations of the UK system, the Court imposed a moral brake and declared that the right being discussed is not an absolute right, but one that involves the courts deciding the situation from the balancing angle. The court noted that the right to privacy will have to be balanced with the right to know of the public, the freedom of the press and the historical record-keeping (*Justice K. S. Puttaswamy v. Union of India*, 2017).

Since *Puttaswamy*, Indian High Courts have been flooded with writ petitions from acquitted individuals demanding the redaction or delinking of their names from digital repositories. The resulting jurisprudence has been highly fragmented, reflecting a system trapped between its adversarial roots and its new inquisitorial privacy aspirations. India's strong digital transformation has outpaced its legislative privacy frameworks; leaving the judiciary to deal with the resulting problems of the digital panopticon retroactively (Bhandari & Sircar, 2017).

The Delhi High Court took a notably progressive stance in *Jorawar Singh Mundy v. UOI* and subsequent 2026 orders. It, to some extent, acknowledged the significance of a legal technicality by distinguishing between "erasure" and "de-indexing." By ordering Google to de-index, the URLs of the acquitted persons, the Court tried to protect the individual's digital record while not altering the essential public information.

On the other hand, Madras HC has gone to the other extreme and followed a purely adversarial and cautious attitude in *Karthick Theodore v. Registrar General*, Madras High Court (2024). The petitioner was acquitted of the criminal charge. He wanted to have his name removed from the judgment that was available on Indian Kanoon. The Madras High Court turned down the appeal on the ground that a court of record cannot, for just reasons of protecting an individual's digital footprint, alter or redact its own judgments after pronouncement. According to the Court, doing so will not only compromise the sanctity of the judicial record but also its historical accuracy (*Karthick Theodore v. Registrar General*, 2024).

The SC later stayed this ruling of the Madras HC (*Registrar General, Madras High Court v. Karthick Theodore*, 2024). Chief Justice D. Y. Chandrachud pointed out that a judgment once pronounced, automatically becomes a "public document." "Therefore, the precise constitutional boundaries of the Right to be Forgotten with regard to official court documents and whether High Courts have the power to order the redaction or de-indexing of their own judgments are, at present, *sub judice* before the Supreme Court.

The legislative attempt to resolve this friction remains similarly inadequate for court records. India passed the Digital Personal Data Protection Act (DPDPA) in 2023, which made the "Right to Erasure of Personal Data" a statutory right under Section 12(3) for data fiduciaries. Nevertheless, Section 17(1)(b) of the Act, which was further detailed by the DPDP Rules issued in November 2025, firmly declares that the Act is not applicable to the processing of personal data by any court or tribunal as would be required for the performance

of its judicial functions (Digital Personal Data Protection Act, 2023).

By legislatively excluding judges from the statutory Right to Erasure, the DPDPA misses the opportunity to provide a systemic solution to people's exposure in the continuous surveillance situation of public court records. It essentially leaves people at the mercy of the judges' natural constitutional powers through the writ jurisdiction, in other words, they do not have a statutory right which they can rely on predictably. India does attempt to strike a balance between these rights but does so in a reactive, ad hoc manner without the structural amnesia of the European inquisitorial model and the absence of predictable statutory guidelines, like the UK's RO Act, 1974.

Suggestions and the Way Forward

Drawing from the comparative study of the inquisitorial system of data-masking and the adversarial system of transparency, this paper suggests the following structural changes:

- India must enact legislation similar to the UK's RO Act 1974. This statute should clearly set a period after which minor convictions or acquittals will be considered 'spent'. Once a record is attested to be spent, the individual will be statutorily protected against getting to disclose it for purposes of the civil (like employment or housing), and digital platforms will be legally barred from giving prominence to such records in search algorithms.
- The solution is to mandate "de-indexing" rather than "erasure." The original judgment will still be available and accessible for legal researchers in the official court archives. However, commercial search engines will be given the legal obligation to remove from their algorithmic search results the name of the acquitted person, thereby practically hiding the record from the ordinary public.
- Those platforms which publish judicial records should rightly be made to follow the algorithmic anonymization rules. After a trial ends, especially when the accused are left free or the case itself is declared void their names should be regularly hidden or changed into pseudonyms (like "A v. State") before the decision is made available on the public internet. This way their digital footprint is protected whilst the legal principle of the case stays available to everyone.
- The hugely broad exemption of judiciary granted under Section 17 of the DPDPA (2023) should: a) not be unlimited; b) be reasonable; \... Executive and Parliament should, in fact, have a say. Although exemptions will be necessary for courts to be able to do their work during trials, the Act ought to be revised to legislate that the judiciary draws up special "data retention and minimization" norms for digital archiving after trials. The judiciary cannot remain entirely exempt from the constitutional privacy standards it established in *Puttaswamy* (2017).

Conclusion

The key juridical difference between inquisitorial and adversarial systems of law essentially comes down to one issue: who is in charge of telling the story of a former offender in the era of the internet? As this paper points out, the conversion of court records into digital form has changed the principle of open justice in democratic societies, turning it into an instrument of continuous, outside-of-court punishment. A constitutional system that always remembers is a system that can neither forgive nor rehabilitate. When past wrong-doings or innocent victims records stay permanently accessible by means of algorithmic search machines, then the government will unintentionally be creating a digital panopticon, which means that the accused are being divested of their humanity and their ability for social re-entry (Mayer-Schönberger, 2009; Solove, 2003).

In short, the European inquisitorial model presents the GDPR as a very strong protection for human

dignity, while common law countries are understandably worried that making digital forgetfulness a principle could lead to the decline of democratic accountability. Yet indeed India's case shows how the adversarial way without laws for protection is neither possible nor effective. By adopting the selective de-indexing procedures, algorithmic anonymization, and a formal timeline for spent convictions, adversarial democracies will be able to safeguard the privacy of the accused while at the same time preserving the official court record. Justice, in fact, in the digital world must consist in a legal system that can adequately remember the law but, at the same time, be kind enough to forget the person.

References

- Bhandari, V., & Sircar, O. (2017). Privacy and the Right to be Forgotten in India. *Indian Law Review*, 1(2), 202--228.
- Court of Justice of the European Union. (2014). *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (Case C-131/12).
- Delhi High Court. (2021). *Jorawar Singh Mundy v. Union of India*, W.P.(C) 3918/2021.
- Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
- European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union*, L 119/1.
- High Court of Justice [UK]. (2018). *NT 1 & NT 2 v Google LLC*, EWHC 799 (QB).
- Jacobs, J. B. (2015). *The Eternal Criminal Record*. Harvard University Press.
- Madras High Court. (2024). *Karthick Theodore v. Registrar General, Madras High Court*, W.P. No. 4600 of 2024.
- Mayer-Schönberger, V. (2009). *Delete: The Virtue of Forgetting in the Digital Age*. Princeton University Press.
- Rehabilitation of Offenders Act 1974, c. 53 (UK).
- Rustad, M. L., & Kulevska, S. (2015). Reconceptualizing the right to be forgotten to enable transatlantic data flow. *Harvard Journal of Law & Technology*, 28(2), 349--417.
- Solove, D. J. (2003). The virtues of knowing less: Justifying privacy protections against disclosure. *Duke Law Journal*, 53(3), 967--1065.
- Supreme Court of India. (2017). *Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors.*, (2017) 10 SCC 1.
- Supreme Court of India. (2024). *Registrar General, Madras High Court v. Karthick Theodore*, SLP (C) No. 15311/2024 (Order dated July 24, 2024).
- Townend, J. (2017). Closed data: Defamation, privacy and the limits of the open justice principle. *Journal of Media Law*, 9(1), 30--44.
- Whitman, J. Q. (2004). The two western cultures of privacy: Dignity versus liberty. *The Yale Law Journal*, 113(6), 1151--1221.