# DATA PRIVACY AND REPUTATIONAL HARM (PRIVACY IN THE DIGITAL AGE)

*by*

Ms.Antashree Nandy

BALLB, LLM, MA in Public Policy and Governance

## ABSTRACT

The world of information and communication technology (ICT) is constantly evolving, leading to unprecedented advantages and opportunities that stem from global connectivity. As a result, the way we share information, communicate with each other, and live our lives has been completely revolutionized by technological advancements. However, a major challenge accompanies these immense benefits -- ensuring digital privacy and cybersecurity remain intact. Social media has become an integral part of daily life in various domains. In the realm of media, people use it to share text, images and messages while businesses employ online surveys, marketing tactics and customer targeting to advance their agendas. Due to its widespread adoption by Internet users today we consider social networking media as a representation of present internet culture. While sharing information on these platforms is convenient there are real privacy and security concerns that must be addressed, particularly with regard to sensitive user data which requires confidential treatment.

The relationship between people and technology is complex and twofold. While ICT has enabled unprecedented connectivity, information access, and communication across boundaries, it also raises concerns about personal data collection, usage, misuse and poses challenges to digital asset security. This paper delves into the significance of safeguarding personal information by exploring various risks such as malware attacks or phishing scams leading to data breaches; workplace privacy issues; legal frameworks governing digital privacy protection; and emerging technologies transforming this environment. Additionally, it examines legislation from different jurisdictions pertaining to these matters. Social media's ascendance has transformed communication channels but created apprehensions about online reputation management and user privacy rights. In essence, the study focuses on the conflicting demands arising from balancing these two dynamics while scrutinizing how regulatory mechanisms can resolve them. Users' entitlements are crucial in determining who accesses their sensitive confidential particulars. However, social networking sites face hurdles in providing tools for users wanting control over their web image.

Journal of Multi-Disciplinary Legal Research



Journal of Multi-Disciplinary Legal Research | Licensed under CC BY 4.0 — https://creativecommons.org/licenses/by/4.0/ | DOI: 10.5281/zenodo.22879698 | Title: Data Privacy And Reputational Harm (Privacy In The Digital Age)

**Research Questions**

1. How do existing legal frameworks pertaining to data privacy and freedom of expression intersect with online reputation management on social media platforms?

2. To what extent do social media platforms effectively balance user privacy and online reputation management functionalities, ensuring both individual rights and a healthy online environment?

**Introduction**

Living in a connected world has brought about unprecedented advantages and opportunities due to rapid advancements in the field of information and communication technology (ICT). This technological evolution has revolutionized how we share information, interact with each other, as well as carry out our daily activities. However, these benefits also come with significant challenges; most notably, safeguarding digital privacy and security. Data plays an essential role in determining socioeconomic activities following the application of emerging technologies. This current paradigm showcases distinct characteristics such as increased global connectivity and transparency alongside higher numbers of qualified individuals required for functioning frameworks continuously updating standards and protocols across various interfaces and devices worldwide. This shift comes alongside ethical and professional hurdles revolving around protecting ownership interests associated with securing personal and private data while ensuring all parties' right to confidentiality is not neglected.1

The issue surrounding data protection concerns gained momentum simultaneously with computer systems beginning to transfer large swathes of electronic records spanning several decades, particularly relevant for progressive societies emphasizing fairness and integrity.2 Today more than ever before, the importance attached to digital privacy rights is paramount, due to the constant entanglement of various digital devices and platforms and the increasing transparency movement and interdependence between global stakeholders. Digital privacy connotes the protection accorded to personal information alongside electronic data communication, preventing unwarranted access and misuse by unauthorized parties. It requires stringent compliance standards as it encompasses fundamental rights that cover the essential aspects of human liberties. Protecting digital privacy rights is crucial, not only from a convenience or preference perspective but also for securing defence against possible threats in cyberspace.

The ability of civilizations to transform themselves by generating and manipulating ideas, culture, social interactions as well as tangible objects is embodied in technology. It is an activity that has significant societal implications which are inevitably linked with privacy considerations. People's perceptions regarding privacy are swayed by technology while their

1 Peter Carey, **Data Protection: A Practical Guide to UK and EU Law** (2nd edn, Oxford University Press 2004) 23.

2 Carey (n 1).

views on this vital aspect influence technological progress considerably. There exists a universally acknowledged belief about human rights such as freedom of speech and expression along with association alongside personal data protection being necessary for ensuring individual integrity.3

India's scale of digital connectivity amplifies these concerns considerably. According to the Telecom Regulatory Authority of India (TRAI), the total number of internet subscribers in India reached approximately 970 million as of December 2024, with broadband subscribers accounting for nearly 945 million of that figure.4 The Internet and Mobile Association of India (IAMAI) reported active internet users at 886 million as of 2024, with rural India surpassing urban India in total user numbers for the first time, indicating that the privacy challenge is no longer confined to technologically sophisticated urban populations.5 This explosive expansion of connectivity, occurring largely through mobile devices with limited user awareness of data collection practices, makes robust and accessible legal frameworks not merely aspirational but operationally urgent.

**The Evolving Landscape of Digital Privacy**

Our understanding of privacy has shifted over time, with varying levels of recognition and importance placed on it depending on different situations. Moreover, other factors such as security or societal welfare often take precedence over the value given to privacy. Unfortunately, there is a lack of concrete empirical data regarding people's attitudes towards various aspects of private behaviour in real-life scenarios. Empirical research is necessary to understand people's perceptions of privacy and its value within fundamental rights. However, the concept of privacy has transformed due to the digital revolution. Digital privacy ensures that personal information like financial details, addresses or phone numbers remain confidential and are not misused by others for malicious purposes such as fraud and identity theft. Moreover, in today's world where online presence impacts one's social image, blogs and professional networking sites influence how others perceive us, but without proper digital protection users may become victims. Targeted abuse including cyberbullying could harm reputations which can lead to perpetrating more harassment against an individual.

Journal of Multi-Disciplinary Legal Research

3 Global Internet Liberty Campaign, 'Privacy and Human Rights: An International Survey of Privacy Laws and Developments' (gilc.org, 2022) <http://gilc.org/privacy/survey/intro.html> accessed 13 September 2026.

4 Telecom Regulatory Authority of India, 'Indian Telecom Services Performance Indicator Report: Quarter Ending December 31, 2024' (TRAI 2025) <https://www.trai.gov.in> accessed 13 September 2026; see also 'Urban Internet Penetration Exceeds 111%, Rural Lagging at 44.99%: TRAI Report' **AdGully** (24 April 2025) <https://www.adgully.com/post/1049/urban-internet-penetration-exceeds-111-rural-lagging-at-4499-trai-report> accessed 13 September 2026.

5 IAMAI and Kantar, 'Internet in India 2024' (Internet and Mobile Association of India, 2024) <https://www.iamai.in/sites/default/files/research/Kantar_%20IAMAI%20report_2024_.pdf> accessed 13 September 2026.

The scale of cybersecurity incidents in India provides measurable evidence of this challenge. According to data presented by the Minister of State for Electronics and Information Technology in the Lok Sabha, the Indian Computer Emergency Response Team (CERT-In) recorded 1,592,917 cybersecurity incidents in 2023 alone, representing a nearly fourfold increase from the 394,499 incidents recorded in 2019.[6] Incidents targeting government organizations specifically numbered 204,844 in 2023, up from 85,797 in 2019. These figures demonstrate that the threat landscape for digital privacy in India is not theoretical but represents an accelerating and empirically documented trend, underscoring the need for adaptive legal frameworks capable of responding at the required scale.

Privacy concerns extend beyond just defamation cases under tort laws; a UK High Court decision confirmed this intertwine while discussing **Sir Cliff Richard OBE v BBC and South Yorkshire Police**[7], ruling that a person's reputation requires safeguarding along with their right to keep private facts from being publicly disclosed because reputational risk arises at the boundary between the law of confidentiality on one hand and the law of libel on the other. As managing your own online persona elevates brand management, limiting harmful exposure is best achieved through ensuring sensible controls around data and information, allowing individuals to be confident in maintaining a good standing offline as well.

**User Privacy: Protecting Personal Data**

The constant evolution of the internet's ability to produce, aggregate, exchange and analyse data has significantly impacted personal data security. Even harmless information such as IP addresses and search queries can be analysed to identify individuals and unearth their private details. With each usage on various online platforms like social networking sites or cookie-based surfing patterns, new user-related information is generated without proper knowledge about its relevance. Personal privacy exposed during a data breach could result in identity theft while cyber attacks may tarnish one's reputation through harassment or bullying cases that are becoming more prevalent especially among teenagers.

Journal of Multi-Disciplinary Legal Research

In the world of information and communication technology (ICT), safeguarding the privacy and data of individuals as well as organizations is reliant on having a legal and regulatory system in place. Such rules aim to establish guidelines, set benchmarks, recommend measures for digital security while administering penalties against violators infringing upon such standards.

---

6 Jitin Prasada (Minister of State for Electronics and Information Technology), Reply in Lok Sabha (December 2024), reported in 'India's Cybersecurity Incidents Hit 1.59 Million in 2023: CERT-In' **APAC News Network** (7 December 2024) <https://apacnewsnetwork.com/2024/12/indias-cybersecurity-incidents-hit-1-59-million-in-2023-cert-in/> accessed 13 September 2026.

7 [2018] EWHC 1837 (Ch).

The General Data Protection Regulation (GDPR)8 is a comprehensive data protection law in the European Union that gives individuals more control over their personal information through strict guidelines for processing it. The GDPR focuses on identifying personal data, which includes sensitive categories such as race or ethnicity, political opinions, religion, trade union membership, genetic and biometric details, health records and sexual orientation. It applies to all organizations that act as controllers or processors of this critical type of information. Online reputation management can benefit from various rights granted under the GDPR relating to an individual's personal data. These include: (1) Right of Access (Article 15): Individuals have the right to view their own information held by platforms and learn how they are using it; (2) Right to Rectification (Article 16): Users may request updates be made regarding incomplete or inaccurate personal information about themselves.

Article 17, also known as the right to erasure, empowers individuals with the ability to request deletion of their personal information in specific circumstances, for example when it is no longer necessary for its intended purpose or if outdated data could potentially harm one's online reputation in terms of digital identity management. This provision permits removal requests concerning irrelevant and inaccurate information that has lost relevance over time.

The financial and reputational consequences of inadequate data protection are substantial and well documented at the Indian level. According to IBM's 2024 Cost of a Data Breach Report, the average cost of a data breach in India reached an all-time high of INR 195 million (approximately INR 19.5 crore) in 2024, representing a 39 percent increase since 2020.9 The report identified that costs attributable to lost business, which include operational downtime, customer attrition, and reputational damage, increased by nearly 45 percent year-on-year. These figures establish that data breaches carry consequences that extend well beyond immediate legal penalties and reinforce the case for proactive compliance with data protection standards rather than reactive enforcement.

Journal of Multi-Disciplinary Legal Research

Cambridge Analytica, a political consulting firm, came under fire during the 2018 Facebook scandal10 for improperly accessing and using millions of users' personal information without permission. This breached trust between Facebook and its users led to concerns about data

8 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, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

9 IBM, 'IBM Report: Escalating Data Breach Disruption Pushes Average Cost of a Data Breach in India to All-Time High of INR 195 Million in 2024' (IBM Newsroom, 31 July 2024) <https://in.newsroom.ibm.com/2024-07-31-IBM-Report-Escalating-Data-Breach-Disruption-Pushes-Average-Cost-of-a-Data-Breach-in-India-to-All-Time-High-of-INR-195-Million-in-2024> accessed 13 September 2026.

10 'History of the Cambridge Analytica Controversy' (Bipartisan Policy Center) <https://bipartisanpolicy.org> accessed 13 September 2026.

privacy and user control on social media sites. Cambridge Analytica obtained this sensitive data through unauthorized methods such as surveying by university researcher Aleksandr Kogan or mining it from their own platform's users, resulting in electoral and political purposes that were not authorized by Facebook officials. As a result of these allegations, there was a significant drop in stock prices accompanied by heightened scrutiny from regulators around the world, leading them to require strict regulations regarding personal user data protection. Eventually an auditor was appointed to investigate. European Union decisions mandating GDPR enforcement across Europe impose penalties that, for the most serious violations, can include fines of up to EUR 20 million, or 4 per cent of the organization's total global annual turnover of the preceding financial year, whichever is higher -- amounts that have become more frequently imposed among larger organizations operating online worldwide.

On the other side, the California Consumer Privacy Act (CCPA) provides specific rights to residents of California in regard to their personal information and its use by businesses. Its success has set a precedent for similar privacy laws at state levels. In today's world where social media can make or break a brand with just one negative post, corporations must be proactive in managing all aspects of their online presence.

The infamous 2013 case11 involving public relations executive Justine Sacco serves as a stark reminder of how harmful online content can have long-lasting fallout on an individual's reputation and professional career. While boarding her flight to South Africa that December, Sacco sent out an inflammatory racist message which quickly gained traction across various platforms, ultimately costing her her position. For the Justine Sacco case,12 even though it is not a legal matter, there are critical ethical and legal inquiries raised. It raises concerns about how to balance potential online harassment against free speech rights. Even though insulting in nature, Sacco's tweet did not present an immediate threat, making it challenging to differentiate protected versus unprotected language on social media platforms.

Journal of Multi-Disciplinary Legal Research

**Online Reputation in Digital Age**

Maintaining a positive online presence is essential in today's digital age for self-expression, networking, and personal branding. However, it also comes with risks such as data breaches or leaks that expose personal information and cyberbullying that can lead to character assassination. To uphold trust in the virtual world, individuals should regularly adjust their privacy settings and safeguard their sensitive data by utilising strong passwords, two-factor authentication methods while practising secure online practices. Dealing with defamatory content on social media platforms brings unique challenges in terms of the speed at which misinformation is spread by these channels, leading to irreversible harm within a brief time.

11 Josh Bernoff and Ted Schadler, 'Empowered' (2010) 88(7-8) **Harvard Business Review** 94, 95.

12 'Justine Sacco Case Study' (Calameo) <https://www.calameo.com/books/005391603a9350eb6ebbb> accessed 13 September 2026.

In **Shreya Singhal v Union of India**13, the Supreme Court of India struck down Section 66A of the Information Technology Act, 2000 as unconstitutional, holding that it violated citizens' fundamental right to freedom of speech and expression under Article 19(1)(a) of the Constitution. Section 66E of the IT Act proposes several defining principles when sharing private images, including capturing, transmitting, or publishing without the permission of the victim, and specifically relating to intimate parts. Possible penalties include fines extending to ten lakh rupees and imprisonment of three years at minimum. Under Section 67, those who publish or transmit obscene and pornographic information electronically face a maximum sentence of three years imprisonment plus a five lakh rupee fine; repeat offenders could receive up to ten years' imprisonment and even higher fines. Additionally, any breach of secrecy or privacy falls under punishment under Section 72.

The nexus between data breaches and online reputation harm has been documented through several high-profile incidents in India. A cybersecurity review by the Internet Freedom Foundation for the third quarter of 2024 highlighted the BSNL data breach and the Star Health data leak as among the most significant incidents of that period, each involving the unauthorized exposure of sensitive personal data belonging to millions of Indian users.14 The review noted that such incidents raise serious concerns about the detection and response capabilities of India's cybersecurity authorities. These breaches directly create the conditions for online reputation harm, as individuals lose control over personal information that can be weaponized for targeted harassment, identity theft, and sustained character assassination across digital platforms.

**Online Reputation Management and the DPDP Act: An Intersection of Freedom of Expression**

In today's world, virtually everything and everyone generates a digital trail. Whether we log into our preferred online platform or engage in financial transactions via electronic banking channels, or enter sensitive information on government portals, every activity leaves some form of an identifiable imprint that can be traced back to us. While the rapid progress in the digital space results in countless breakthroughs and possibilities, it also exposes us to various cyber risks with tangible impacts outside cyberspace.

In 1995, VSNL brought the internet to India and ignited digital progress in a growing nation. Over two decades, this progress transformed into an essential element for major industries, including government operations, making it a crucial component of the country's

13 Global Freedom of Expression, Columbia University, 'Shreya Singhal v Union of India' <https://globalfreedomofexpression.columbia.edu/cases/shreya-singhal-v-union-of-india/> accessed 13 September 2026.

14 Internet Freedom Foundation, 'IFF's Cybersecurity Report for the Third Quarter of 2024' (IFF, November 2024) <https://internetfreedom.in/iffs-cybersecurity-report-for-the-third-quarter-of-2024/> accessed 13 September 2026.

infrastructure. The urgency to digitize information with convenience and optimal welfare for citizens necessitated comprehensive digital protection frameworks.

Sensitive data is shielded from potential threats such as loss, manipulation and misuse through digital protection. The Constitution's Article 21 addresses an individual's Right to Life and Personal Liberty. In **Justice K.S. Puttaswamy v Union of India** (2017), the Supreme Court of India held the right to privacy to be a fundamental right under Article 21, while also recognising that information pertaining to an individual must be safeguarded in order for privacy rights regarding access to be ensured.15

The Digital Personal Data Protection Act, 2023 (DPDP Act) guarantees people the essential opportunity to control their online reputation through access, correction, and erasure of their personal data. With this legislation in place, individuals are empowered to inquire about information regarding their data held by a data fiduciary and request modifications for any inaccurate or deficient records they may encounter. Additionally, specific circumstances such as withdrawn consent or unauthorised processing warrant legal deletion requests from concerned parties.

The Right of Access (Section 11) grants individuals the ability to access their personal information, which is held by data fiduciaries like social media platforms. They can ascertain why this information is being processed and identify any false or harmful content that could harm their online reputation.

Similarly, Section 12 enshrines the Right to Correction and Erasure, where an individual may request a data fiduciary correct incomplete or inaccurate personal details. This rectification and erasure power affords people greater control over potentially damaging material about themselves that might undermine their image. An individual may request erasure under Section 12 where, for instance, the original purpose of processing has been fulfilled or consent has been withdrawn.

Journal of Multi-Disciplinary Legal Research

It is important to note that the DPDP Act, 2023 does not create a standalone 'right to be forgotten' as a separately named right. Section 18 of the Act is the provision establishing the Data Protection Board of India, the adjudicatory body responsible for receiving and investigating complaints and imposing financial penalties. The right to erasure, which is conceptually closest to the GDPR's Article 17, is governed by Section 12(3) of the DPDP Act, and is addressed alongside the right to correction within the same provision.

Data privacy has become a critical concern as we share more private information across borders. Though the EU has enacted strict legislation, and an agreement between the US and EU is in place to protect data, India's laws are still developing. While it is expected that regulations will eventually be strengthened in India to better secure personal information, there are pressing issues facing lawmakers beyond just passing new rules. Even if stronger protections were put into effect, effective implementation requires swift action against

15 Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.

wrongdoing and certain penalties for non-compliance. Without addressing systemic problems with enforcement, including court delays leading to unresolved cases, any legal efforts may fall short of their intended goal.

The financial stakes of the DPDP Act's enforcement framework are substantial and provide important context for understanding compliance incentives. According to reporting by The Tribune, entities failing to implement reasonable data security safeguards may face penalties of up to INR 250 crore, while failure to notify the Data Protection Board and affected individuals following a personal data breach carries separate penalties.16 These regulatory penalties are set against a backdrop of rapidly increasing breach costs. IBM's 2025 Cost of a Data Breach Report found that the average organizational cost of a data breach in India reached an all-time high of INR 220 million in 2025, a 13 percent increase from the prior year, with phishing identified as the leading attack vector at 18 percent of incidents.17 Taken together, these figures indicate that the financial cost of a breach in India consistently and significantly exceeds the cost of proactive compliance measures, making the economic argument for data protection investment increasingly difficult to resist.

**Conclusion**

Concerns surrounding privacy have not been generated by modern technology. Even in the absence of online social networks, communication takes place within a framework that still exists through social networks. Unfortunately, sharing information informally with colleagues or friends can lead to unfavourable outcomes when it is leaked and spread as rumours or gossip. Nonetheless, the significant number of individuals utilising these platforms presents alternative features where anyone with basic technological knowledge could access international networks. In today's age dominated by Information and Communication Technology (ICT), digital privacy and security play pivotal roles necessitating an approach balancing individual rights alongside regulatory oversight and innovation factors, favourably for all parties concerned. Continuous adaptation for vigilance purposes must follow due to evolving threats inspired via innovative technologies, aimed at safeguarding our digital lives from unauthorized manipulation. Using contemporary tools requires responsible use, guaranteed only through ICT literacy, as new legal frameworks become necessary while protecting user data remains everyone's primary obligation even regarding newly produced high-tech systems requiring future regulation considerations

16 'Data Protection Bill Tabled in Lok Sabha; Entities Violating Norms to Face Penalty of up to Rs 250 Crore' **The Tribune** (3 August 2023) <https://www.tribuneindia.com/news/business/data-protection-bill-tabled-in-lok-sabha-entities-violating-norms-to-face-penalty-of-up-to-rs-250-crore-531763> accessed 13 September 2026.

17 IBM, 'India Records Highest Average Cost of a Data Breach at INR 220 million in 2025: IBM Report' (IBM Newsroom, 7 August 2025) <https://in.newsroom.ibm.com/2025-08-07-India-Records-Highest-Average-Cost-of-a-Data-Breach-IBM> accessed 13 September 2026.

promoting safe exploitation processes beneficial globally without neglecting strategic partnerships essential for worldwide models.

