International Journal of Advanced Research and Development
www.multistudiesjournal.com
ISSN: 2455-4030
Received: 01-06-2025, Accepted: 01-07-2025, Published: 16-08-2025
Volume 10, Issue 3, 2025, Page No. 25-30

Position of data protection in Indian and International law fraternity: Future perspective/emerging trends in data privacy (DPDP Act, 2023)

Surendra Singh Chundawat[1], Laxmi Bhati[2]
[1] Assistant Professor, Department of Law, Janardan Rai Nagar Rajasthan Vidyapeeth (Deemed to be University) Udaipur, Rajasthan, India
[2] Research Scholar, Department of Law, Janardan Rai Nagar Rajasthan Vidyapeeth (Deemed to be University) Udaipur, Rajasthan, India

Abstract
To understand the concept of the data protection, it is important that we realise the relationship between the data protection and law fraternity. The law fraternity consisting of lawyers, judges and teachers, has to be conscious of the fact that data protection has a huge implication on the society which starts from the individual citizen and extends to the large units like State, Countries, International Organizations etc. In case the concept of data protection has to be understood by an example, the classic example would be jurisprudential rights emanating out of the day-to-day conduct of law fraternity. It is important to note that the law fraternity is handling a large component of data, and the pulls and pressures, which arise out of gaining maximum transparency on one side and giving maximum privacy to the litigant/citizen on the other side, is a tug of war, which the law fraternity is confronted with and has to resolve. Once the concept of data handling by the law fraternity is deeply studied it would give a wholesome example as to how the other components of the society will be in a position to handle the data.

Keywords: Data privacy rights, data privacy act, personal data protection, personal information, laws, rules & regulations, court

Introduction

The data protection has become significant right of the common citizen and transparency requires maximum data to be displayed by any organization for the common good of the society, as we speak of the tussle between the two ends, the real challenge to the society gets highlighted and resolving the same becomes an issue which would help the other segments of society in law to meet the complex issues. The citizens or the smaller units of the society submit a large number of data of varied nature and expect that their data is fairly controlled by the law fraternity. The data given to the legal system is so humongous that in case the fraternity fails to consume it in a rational, transparent, widely usable and optimizing manner while balancing the act of privacy, the creditability of the system is likely to be at stake. Any imbalance in dealing with such responsibility casted upon the law fraternity will go a long way to determine the health of the data usage by the fraternity.

One way to generalize India's current state of court record access is as follows

1. Unless and to the extent that laws or court rules grant such a right, the general public (non-parties) does not automatically have the right to examine court records.
2. The main source of regulations controlling the public's (non-parties') access to documents is the court's rules.
3. When authorization is needed to view these records, the registrar or the court will use their discretion to weigh competing interests such the right to privacy, secrecy, and a fair trial. The court's deliberations revolve around the idea of transparent justice. Unrestricted access to all court records is not the same as open justice. Any access policy should balance the conflicting factors by designating a subset of documents that are typically handled in a way that permits unrestricted access, and by giving all other documents more examination before granting non-parties access to them.

Documents in the First Category should be those that are available to the public without a judge's approval. This should include records that are crucial to the administration of justice and to which the public should have unrestricted access. These would contain the fundamental records of any court decision: those that explain the nature of the dispute, the arguments put up by each side, and the process by which the court resolves it. Currently, this covers access to live courtroom proceedings as well as decisions and orders made or given in public. The judiciary must also consider whether it would be possible to make future releases of other types of documents—like pleadings and transcriptions— available to the public. This necessitates modifications to court rules and regulations, which must be made after consultation. Furthermore, it will be necessary to consider when such documents will be accessible. To maintain the integrity of the legal system, for instance, pleadings containing disputed facts should only be made public after the case is resolved. Despite this, occasionally information found in the first category of documents may be inappropriate to make public. Consequently, only to the extent required in a particular situation should the court retain the authority to limit access or set limits on the use of the material accessed, either on a party's request or on its own action. Moreover, it should not be the responsibility of the court to go through the records looking for material that shouldn't be shared. Rather, it should be the parties' and their attorneys' responsibility to bring such material to the court's notice by way of an application.

All remaining documents that do not fit into the first category will be included in the second category, and their unavailability won't significantly hinder one's ability to comprehend the court's ruling in a particular case. This will include affidavits, exhibits, materials offered as evidence, including judgments or orders rendered in camera or prohibited from being reported by statute or court order. A significant and justifiable interest in the case at hand, as well as approval from the court, are required in order to access this type of material.

a. Standards for Creating Privacy-Related Exceptions to the Open Courts Doctrine Given that the open courts doctrine will be the norm in the legal system, data rules ought to address privacy concerns by establishing exceptions to the doctrine. These can be determined by applying a variety of criteria to impose specific limitations on the data release. The following are some general guidelines that can direct the creation of such a policy:

1 Taking "content and context" into consideration is essential when creating policy for material related to both criminal and civil justice. Information found in court documents needs to be evaluated according to its type and the context in which it occurs. Judicial records may contain "large or small" information, including a name or the total of several components (i.e., papers, like arrest reports, indictments, pleas, and court orders). Every data piece in the court records needs to have privacy policies applied to it, wherever that is possible. Every component must also be considered in its context. For instance, it might be decided that broad information about times, locations, and events must be shared with the public and other government agencies, such as the police and prisons. If there is a threat to the safety of a victim, witness, or member of the public, this materialmay not be made available to the public until the inquiry is over, even if it is contained in a document that is part of an ongoing investigation. Similarly, a data element like "address" might generally be considered publicly accessible or disclosable. However, a privacy analysis may conclude that the address is not appropriate for public access and is not suitable for inter-agency exchange if it is the victim's address and appears in the victim statement or a court exhibit.

2 The relationship between an individual and the justice system must be acknowledged by data regulations. In the context of judicial proceedings, it may be useful to consider regulations that serve three audiences:

the internal audience, which includes law enforcement, prosecutors, defense attorneys, judges, court administration, correctional facilities, and vendors who provide technological services to the judiciary (whose contracts must also include their adherence to privacy regulations and associated liabilities);
and the external audience, which includes those actors (such as charged or convicted offenders, plaintiffs, witnesses, or victims) who have a relationship with the justice system but are not an operational part of it.

- The public, which includes members of civil society, journalists, academic researchers, citizens, and businesses in the newly formed legal tech sector, as well as any other individuals or groups with no connection to or involvement in the proceedings. Judicial data regulations must address issues unique to each of these audiences. It is important to highlight that, when thinking about the "internal" audience, there is a propensity to presume that personal data on anyone with a "relationship" to the legal system can be shared freely, provided that the sharing is done for explicit and legitimate purposes. Rules that govern information sharing within the criminal justice system's various entities— such as the police, prosecutors, defense, courts, and prisons—differ from those that govern information sharing when it comes to those outside the system. For instance, public prosecutors, the accused, and their attorney would need access to evidence gathered by police or investigative agencies; yet, these are typically kept confidential.

3. Regulations governing judicial data must take into account a person's standing and function within the legal system. Victims, witnesses, law enforcement officials, judges, court employees, plaintiffs, respondents, attorneys, advocates, defendants, offenders, their families, associates, and anybody else involved in the legal system are among the people whose privacy interests may be impacted by the courts processing their data. The different ways in which these people engage with the courts and the ways in which their personal data is gathered and utilized in the legal system must be taken into consideration by judicial data regulations. Personal information belonging to a convicted criminal, for instance, would be handled differently from that of a witness. Moreover, how personal data gathered for an investigation is handled could be different from how it is gathered and utilized in a case processing system. Depending on their position, function, and connection to the legal system, the stakeholders in this part can access court documents using an indicative framework provided in this section. The sensitivity and specificity of the information sought are further considerations. The duties of the courts, who are the guardians of all the data submitted by the judicial participants, are also highlighted in this section.

b. The Framework for Determining the Degree of Confidentiality and Public Access Permitted to Court Records - Any law managing judicial data must include a mechanism for objectively and consistently striking a balance between the public interest in having judicial data freely accessible and the privacy issues raised by it. This can be accomplished by taking into consideration every feature of the data that affects the requests for transparency, privacy, or both. In some circumstances, particular to legalprocedures, privacy issues and obligations for transparency arise not only from the substance of the information alone but also from the usage of the information in context. A summary of these elements is provided below:

1. The data fields' sensitivity Numerous privacy frameworks, such as the GDPR and the PDP Bill,

define broad categories of data according to how sensitive they are. The level of harm that an individual may experience as a result of the public revelation of such data is used to determine the sensitivity of that data. Different jurisdictions' privacy laws distinguish between personally identifiable information (PII) and other information that allows for the identification of a natural person. PII is protected because, depending on the situation, its use may constitute an invasion of privacy. Many provide a higher level of protection to a kind of "sensitive personal data," which puts the individual who is the subject of that data at significantly more risk should it be made public. A straightforward, standardized method of balancing privacy with transparency is to draw boundaries around data categories according to the principal's possible exposure. This will be necessary as the judiciary transitions to entirely digital procedures inorder to control access and guarantee transparency. Therefore, we address the damage and relevance of identifiers while developing judicial data laws, as well as the necessary modifications to ensure that they do not conflict with the open court's theory.

1. By default, open data First things first, a class of open data must be identified where there is minimal risk of injury or misuse. This covers records and information that will be made available to the public, including statistics about the court system, its laws and regulations, and the majority of administrative data that does not deal with the private or delicate personal information of specific employees. It should also contain all data from court records that do not contain sensitive data, as well as documents and other records from which all data that could be misused has been eliminated. This should contain identifiers for bulk data as well as rulings and orders following the removal of sensitive personal information. Open justice requires that certain types of personally identifiable information (PII) be identified as open data, depending on the context and volume in which it is made available, even though non-sensitive personal data is generally not regarded to be safe to include in open data.

2. **Personal data (PD):** The foundation of that in relation to the data is the relationship that exists between a data unit and a real person. An individual's rights are applicable when data is linked to their identity, as privacy serves as a guarantee for their dignity. It is problematic, nevertheless, to use identifiability as the exclusive basis for limiting access to information under the open court's theory. Although it is helpful, the idea of personally identifiable information as a category for data protection regulation shouldn't serve as the main foundation for regulation in the legal system. In the context of RTI applications, the Supreme Court and other High Courts have rendered decisions on the necessity of balancing the public interest inaccessing information against the privacy of the individuals to whom it relates. According to the Puttuswamy ruling, making personal data public in accordance with the open courts theory is consistent with the fundamental right to privacy and cannot be viewed as a breach of that right. It satisfies the requirements of legality, necessity, and proportionality set forth by the Supreme Court for a valid restriction on the right to private. The requirements of the Code of Civil Procedure, 1906, and the Code of Criminal Procedure, 1971, which mandate that trials be held in public, witness testimony be heard, and judgments be rendered, satisfy the legality requirement. The Constitution's Article 145(4) mandates that decisions made by the Supreme Court be delivered in public. In terms of need, the Puttuswamy ruling's standard is met when data release serves the interests of the just and equitable administration of justice. Restrictions on the right to privacy must be justified by the needs of the state.

3. **Sensitive personal data (SPD):** For a more protected type of data, certain exceptions to the open courts doctrine should be made. Whether or not the data could put data principals at risk of serious harm must be taken into consideration when defining this category. Financial information, health-related information, official identifiers, biometric and genetic data, and official identifiers are among the categories of data that fall under the PDP Bill's sensitive personal data category by default.

However, the definition of sensitive data should not be limited to these narrowly defined categories

1. The ability of the data to cause harm (from fraud to social discrimination),
2. As well as the likelihood that this will happen if the data is made public, are some criteria that can be used to assess if the data is sensitive.
3. The expectation of privacy with respect to specific categories of data, like health information; and
4. The concerns voiced by the majority of citizens, which are significant because the harms that do occur only impact a small portion of the population, making the majority less likely to be concerned about those particular harms.

2. Weighing the precedent value, public interest, and data field sensitivity - The previous point suggested that courts should have the authority to decide whether or not to disclose SPD to the public in court documents. This section will go over the guidelines and methods that can help with these choices. Numerous instances exist where the judge has limited or prohibited the release of SPD in court documents in order to preserve both the right to privacy and the impartial administration of justice. These can aid in ensuring that the privacy restrictions required to accomplish a just and equitable administration of justice are reasonable and well-balanced. Developing consistent, standardized, "bright line" criteria of proportionality is more challenging, though, because privacy and the trade-off between transparency and privacy can be highly contextualized. Think about a scenario where the information concerns personal facts of a person's life and they are being accused of a small-time offense. Should that information be considered evidence in the case that is outlined in a ruling, there would be enough public interest to make it public if doing so would just cause the party involved to feel slightly embarrassed, but not if it would result in a credible and serious threat of violence against them.

Regulations governing judicial data must acknowledge each person's position and function within the legal system—Victims, witnesses, law enforcement, judges, and others whose privacy interests may be impacted by the courts processing their data include employees, respondents, plaintiffs, attorneys, defendants, criminals, their relatives, and anybody else who interacts with the legal system. Regulations governing judicial data must consider the different kinds of interactions these people's interactions with the legal system, how their personal data is gathered, and designed for use in the legal system. For instance, the personal property of a convicted criminal information would be handled differently than the private information of a witness. Additionally, how personal data gathered for an investigation is handled may vary from data gathered and utilized by a case processing system. This section offers an indicative framework that allows different stakeholders to access court records according to their function, role, and connection to the legal system. Other elements consist of the level of detail and sensitivity of the information being sought. Additionally, this section emphasizes the duties of the courts, which are in charge of keeping track of all data supplied by the participants in the legal system.

Access timing, the rules of many High Courts stipulate that in order to ensure the fairness of proceedings, copies of the record, including depositions, pleadings, and other documents are usually only made available to outside parties following the conclusion of proceedings, with the exception of in extraordinary situations where there is a valid reason. This idea ought to be kept in a digital format and included in laws governing judicial data. In other jurisdictions, the extent of public access is determined by considering the stage of a case to records.

For example, Grand jury proceedings are closed to the public and media in the United States. Indictments issued by grand juries and federal and state courts are sealed until an arrest is made. Pre-trial service officers investigate defendants' criminal histories following an arrest or indictment. Backgrounds to help judges determine pre-trial release conditions and bail. Consequently, pre-trial reports are not made public and are intended solely for the judge. All of these guidelines are created to safeguard the integrity of the process and uphold the right to a fair trial.

In the UK, Crown Court judges and magistrates may make pre-trial rulings on the admissibility of evidence, or on points of law relevant to a forthcoming trial, and undertake preparatory hearings in terrorism related cases and other cases such as long, complex or serious cases, and serious fraud cases. Automatic statutory restrictions prevent the reporting of these rulings. These restrictions continue until the trial has been concluded, when they automatically cease to apply.

In some Canadian courts, documents related to bail applications, affidavits, etc. the letters and conditions of release prepared by the court are not available to the public before a judge has heard and decided the bail application. The pre-sentence reports are also not available to the public until a judge has imposed a sentence.

Recently, some courts have started to stream cases live during trials, including the Gujarat and Karnataka High Courts. The phases of live streaming cases where public interest is arguably most crucial are the conclusion of arguments and the announcement of judgment. For all cases that are not heard in camera, these stages are accessible to the general public. But for cases of public importance, every step could be streamed live. Ideally, the court employees will be in charge of using their time to censor sensitive information. The same stage-specific regulations would be applicable in the event of a telecast delay. For non-live cases: streamed, but the court may order that the recording be made available online. Some parts ought to be left out. The privacy hazards that come with live streaming should not discourage litigants or attorneys from using a specific piece of information to bolster their argument in court.

The majority of data protection laws specify the responsibilities of data processors, data fiduciaries, and other comparable positions, to guarantee that their utilization of data does not infringe upon data rights principles. In the legal context, these ought to be reinforced because personal data is already extensively accessible in court documents and ought to stay that way for the benefit of open justice.

Rights of data principals in the judicial context given that the interest of fair administration of justice can conceivably override privacy concerns in certain situations, PD would be made public, and SPD may also be made public, if determined to be of sufficient public importance for example, in PILs, cases involving public officials etc. The data principals that this data pertains to should still have a means of redressing any harm that is done to them through the use of this data.

In order to ensure the equitable administration of justice, judges would have the authority to limit them fairness. Therefore, we advise that a set of data be included in the judicial data regulations protection rights that are appropriately adjusted for the legal system and that codify the circumstances and functions where each right is exempt in the interest of the administration of justice.

These could consist of

1. Rights like the ability to verify that someone else has and is using one's information and the authority to view it;
2. the right to be corrected;
3. the freedom to transfer data; and
4. the right to be forgotten in certain situation.

a. section of the online Pennsylvania Courts system has been compromised by a cyber-attack. Chief Justice Debra Todd of Pennsylvania declared that the compromised system, claiming that sections of the website are consequently, it is not available. The cyber-attack is referred to as a denial of service attack one.

- The US judiciary has seen a dramatic rise in cyber-attacks and the previous years in Europe. In 2019, there were 24 million attempts, versus 9 million of cyber-attack attempts were made in the United States alone in 2016.

Two federal judges on Thursday warned a U.S. Congressional panel that the judiciary's aging computer systems are "vulnerable" to cyber-attacks, creating a risk that hackers could obtain confidential material or draft court decisions like the U.S. Supreme Court abortion opinion leaked earlier this month. The testimony came during a hearing of the U.S. House of Representatives' appropriations

subcommittee on Financial Services and General Government concerning the federal judiciary's $8.6 billion budget request for the 2023 fiscal year.

Victoria's court system has been hit by a ransom ware attack, which an independent expert believes was orchestrated by Russian hackers. A spokesperson for Court Services Victoria (CSV) said hackers accessed an area of the court system's audio-visual archive. That would mean recordings of hearings including witness testimony from highly sensitive cases may have been accessed or stolen. CSV is now trying to notify people whose court appearances have been accessed by hackers, and will today set up a contact centre for people who believe they may have been affected.

That studies about the privacy of data protection in everywhere whether it is India, US, Canada, or any country. In Indian' Constitution citizens have a fundamental right for own privacy in all way. Where's today all data available on online that is why need to be protect all types of data and decrease their risk. Role of judiciary is also most important in data protection on national and international levels court. Many judgments and explain laws related to protection of data. Law does not only require data protection but also by ethics in an era where data is a valuable asset. In the digital age, protecting privacy, fostering trust, and defending human rights all depend on making sure that personal data is handled appropriately. The Indian judiciary has been instrumental in recognizing privacy rights in the absence of a strong statutory framework. The international judiciary, especially the CJEU, has led in enforcing strong, codified protections under the GDPR. With the Digital Personal Data Protection Act, 2023, Indian courts are likely to increasingly interpret and apply statutory principles, possibly converging more with EU-style data jurisprudence.

Landmark Case: Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) The Supreme Court of India unanimously held that the right to privacy is a fundamental right under Article 21 (Right to Life and Personal Liberty) of the Indian Constitution. It laid the foundation for data protection law in India. Recognized informational privacy as a key component. Stressed the need for data minimization, purpose limitation, and consent.

Belgium Case of Facebook Belgian DPA v. Facebook Inc. CJEU, Case C-645/19, Court 2021 The main idea even if Facebook is not based in their nation, National Data Protection Authorities (DPAs) have the authority to file lawsuits against it under certain circumstances. Sufficient Protection According to Schrems cases, courts emphasize that nations that receive data from the EU must have laws providing comparable protections. Proportionality and Data Minimization Mass data retention and indiscriminate surveillance are frequently challenged Digital Rights Ireland Rights of Users People have legally binding rights regarding their data, such as the ability to have it erased, corrected, or consented to Google Spain Cross-Border Enforcement Under the GDPR, DPAs and courts can operate even outside of EU countries Facebook Belgium. Technological Awareness Courts are becoming more aware of and considerate of the ways in which technology such as cloud storage and mobile data affects privacy Carpenter.

Maximillian Schrems and the Data Protection Commissioner v. Facebook Ireland Ltd. Court: Case C-311/18, CJEU 2020 The EU-US Privacy Shield, Safe Harbor's replacement, was declared invalid by the CJEU discovered that US regulations such as FISA 702 did not provide the same level of protection as the GDPR.SCCs (standard contractual clauses) were only upheld if they provided sufficient protection, i.e.

To comprehend the ideas behind data protection and the right to privacy.

To carefully consider the various aspects of data protection law.

To analyze the opinions of several landmark rulings in the areas of privacy and data protection to specify and identify the limitations and rights. In order to evaluate the effects of data theft and the legal measures taken to prevent it, they comprehend the broader ramifications of the battle to control data. Data protection's effect on our country's economy.

To identify the difficulties faced by multinational corporations trying to influence national policy in order to safeguard their interests.

To investigate the tension that exists between public and private control over personal data. That when transferring personal data outside of India, organizations may be required by law to adhere to certain requirements or secure individual consent.

The goal of this regulatory framework is to guarantee that people's right to privacy is upheld even when their data is moved to another country with possibly different data protection laws. That the law may require organizations to implement robust data protection mechanisms, such as encryption and access controls, to safeguard personal data from unauthorized access, breaches, or misuse. These enhanced security measures may contribute to preserving individuals' privacy. These actions support people's right to privacy by encouraging a culture of openness and responsibility among data controllers and processors. The law gives people the ability to exercise their rights, including the ability to view, update, and remove personal data that is kept about them by organizations. The ability of people to safeguard their privacy and make knowledgeable decisions regarding their data may be improved by this empowerment.

Conclusion

In the aforesaid study it becomes clear that data has to be classified & categorised so as to ensure that the feature of common good and complete utilization of such data is secured. It is to be seen that a jurisprudence to be developed in this regard has a credible impact upon the other components of societal organization and thus is what the law fraternity does to consume and deal with the data is likely to be imbibed with the other limbs of society. The common citizen has the highest expectation castinghighresponsibilityuponthe law fraternitytodealt with suchdata categorization. The mightiest organ of law fraternity is itself precedent law and thus the story of legal jurisprudence begins with the data which we know as precedent law. On one hand clarity in law, subjectivity in issues and objectivity in ideas can be achieved only when such data is universally accessible and on other hand lies the challenge to assure a common citizen/litigant that the data provided by him shall be used in a manner not detrimental to the future of such citizen. The citizen’s faith is sacrosanct, behaviour of the lawfraternity shall help us achieve the goal of data control, data protection, data

consumption and data sharing. The law fraternity while dealing with the deep-rooted concepts of transparency vis-a-vis privacy is shoulder with responsibility of society into an era where we can have sustainable dataconsumption in a manner most conducive to the democratic society. Today the challenge before the law fraternity and though we continue to evolve ourselves in a flexible mode to gain strength in the shape of confidence of the data user vis-a-vis data supplier will lead us to a strong nation with credible operation of democratic and constitutional rights.

References

1. Judiciary data. 2021-22 www.cbsnews.com
2. www.nja.gov
3. Federal judiciary vulnerable cyberattack 2022-05-12, www.retuers.com
4. Victoria court system Russian hackers 103272118, www.abc.net.au.in