JUDICIAL DATA REGULATION

DISCUSSION PAPER I

Balancing Open Courts With The Right To Privacy – An Indian Perspective

JULY 2021

DAKSH

ACKNOWLEDGEMENTS

This paper is an independent,
non-commissioned piece of academic work,
authored by Aakanksha Mishra and Siddharth
Mandrekar Rao.

The authors would like to sincerely thank
Surya Prakash B.S. and Leah Verghese for
their able guidance throughout the research
work and for reviewing the paper.

The authors are grateful for the valuable
suggestions of Harish Narasappa, Prashant
Reddy, Smriti Parsheera, Shweta Mohandas
and Malavika Raghavan. Lastly, the authors
would also like to acknowledge the efforts of
Sandhya P.R. and Shruthi Naik at DAKSH in
reviewing and editing the paper.

CONTENTS

CHAPTER 1

INTRODUCTION

'Justice must be done and must be seen to be done' is a fundamental tenet of our legal system. The long-venerated principle of open justice (including open courts) requires that court proceedings must be accessible to the public. In reality, relatively few members of the public have used that open door, and court reporters have acted as the intermediaries between the justice system and the wider community. With the rise of new technologies, the traditional methods of guaranteeing open justice for the community are rapidly changing[1]. Open justice now increasingly means the ability of the community to access information about the courts through the internet. Courts in India, like other institutions, are transforming from largely paper-based systems of processing and record-keeping to digital records, and from primarily locally accessible records to records accessible online via the internet.

Judicial data[2], including court records, exist at the confluence of two strong currents in India. One current is the demand for openness. Since records provide an essential window into the functioning of one of the three pillars of government—the judiciary—citizens are presumed to have a right to inspect them to ensure that courts are exercising their powers competently, fairly and within the limits of their mandate. The other current is privacy. Human dramas are recounted through court records, which includes massive amounts of personal information about the various people involved in a given dispute. And with increased access to online court records, it is only to be expected that the creation and exposure of these accumulated volumes of personal information will give rise to privacy concerns[3]. The loss of "practical obscurity" lies at the heart of the debate about privacy risks from online access to court records.

While a lot has been written about the competing interests of government transparency and personal privacy, the focus on privacy concerns arising out of judicial proceedings and court records has largely been overlooked in this discourse. This paper aims to inform the scholarly and policy discussions about the appropriate balance between public access and privacy in the context of judicial proceedings and judicial data. Chapter II defines judicial data and categorises the various kinds of personal information

[1] Marilyn Warren. 2014.'Open Justice in Technological Age', Monash University Law Review, 40(1): 45- 58.

[2] Defined in Chapter 2

[3] Amanda Conley, Anupam Datta, Helen Nissenbaum & Divya Sharma. 2011. 'Sustaining Privacy and Open Justice in the Transition to Online Court Records: A Multidisciplinary Inquiry,' Maryland Law Review, 71: 722

contained in court records. Chapter III notes that court records present a special challenge for privacy due to the unique doctrines, principles, and institutional arrangements that characterise the judicial process and the judiciary's relationship to information/data. Unlike in many other areas of privacy law, court records are presumptively open to the public. In Chapter IV, after considering the differences between traditional paper-based court records and online access to electronic court records, we dive into the challenges presented by court records in the digital environment and their implications on privacy. In Chapter V, we discuss the legal status and contours of the right to privacy in India in light of the landmark judgement of the Supreme Court of India in *K.S. Puttuswamy v. Union of India*[4]. In Chapter VI, we survey how the principle of open courts and the fundamental right to 19(1)(a) of the Indian Constitution have been balanced with the more recently recognised fundamental right to privacy. In this chapter, we review court decisions on in-camera proceedings, live streaming of court of proceedings, prohibition on publication and reporting as well as the current framework regulating access to court records. We conclude, in Chapter VII, by providing some suggestions for mitigating and minimising potential conflict between the right to know, and the right to privacy in the judicial context.

In this part we review court decisions on in-camera proceedings, live streaming of court of proceedings, prohibition on publication and reporting as well as the current framework regulating access to court records which includes the rules of each court and the Right to Information Act, 2005. We conclude, in Chapter VII, by providing some suggestions for mitigating and minimising potential conflict between the right to know, and the right to privacy, particularly in the judicial context.

[4] K.S. Puttuswamy v. Union of India, 2017 10 SCC 1 decided on 24 August 24 2017 (hereinafter referred to as Puttuswamy I)

CHAPTER 2

PERSONAL INFORMATION IN JUDICIAL DATA

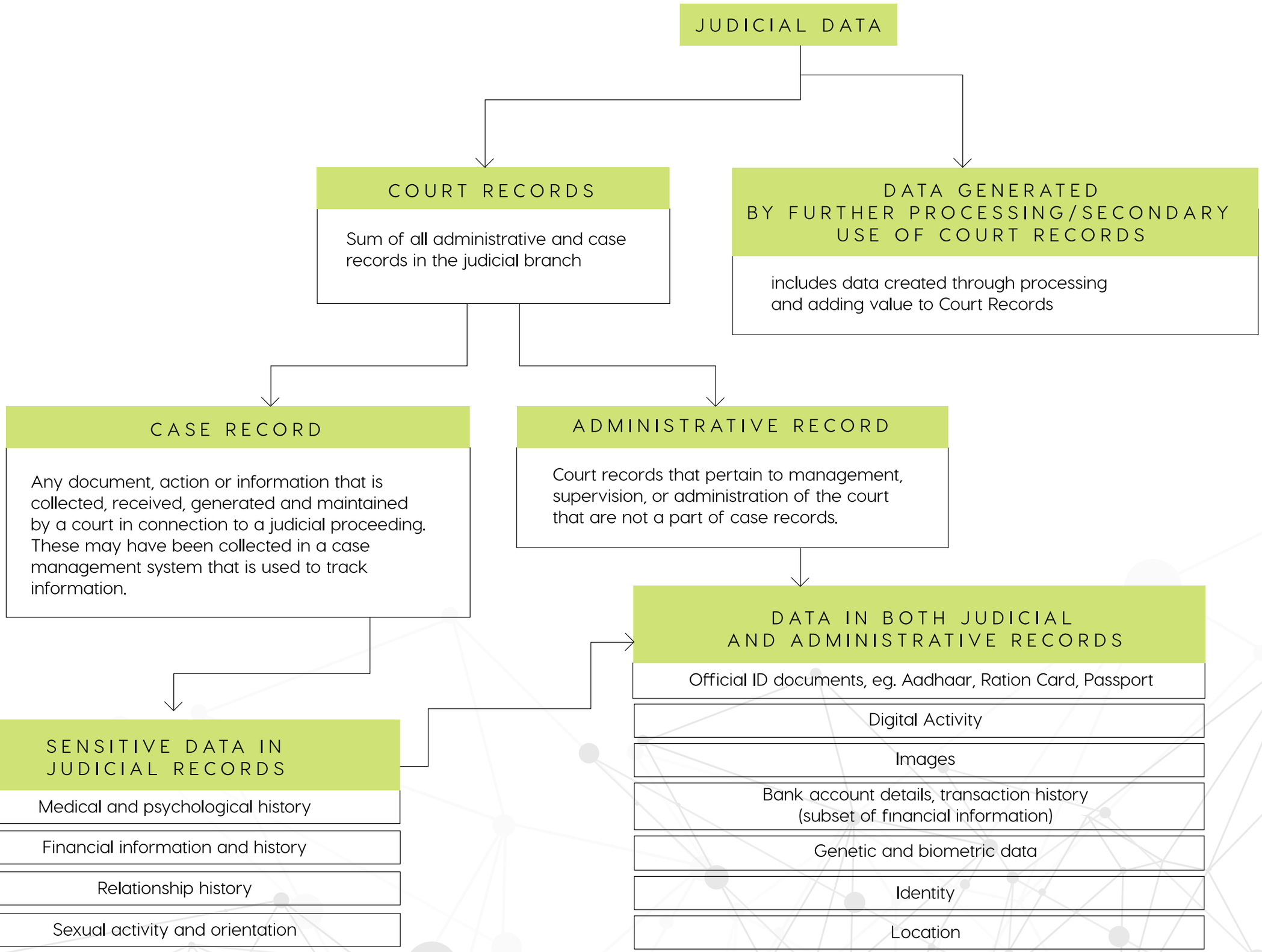
A. WHAT IS JUDICIAL DATA?

Judicial data comprises data generated by the courts and created through processing and adding value to data created by the courts (further processing/ secondary use). For the purpose of this paper, the term 'judicial data' will include both. Judicial data is generated not only over the course of case proceedings (civil, criminal or whatever be its nature) based on facts and information that are submitted by litigants and lawyers, but also includes the court's administrative and financial records, judicial statistics and secondary sources that make use of data generated by the courts such as legal databases and law journals. In *Chief Information Commissioner v. High Court of Gujarat and Another*, the Supreme Court distinguished between 'judicial side' and 'administrative side' information held by the high courts. Judicial side information includes any documents and other information submitted by parties, lawyers, investigation agencies, or any other participant in the case, over the course of a legal case (e.g. pleadings, documents and other materials and memo of grounds raised by the parties), in addition to any information generated by the court which pertains to the case (e.g. orders and judgments, notes of proceedings). In exercise of their powers of superintendence, the high courts may also hold similar information submitted by /called for from subordinate courts and tribunals, which are also considered judicial information.

> "Judicial data is generated not only over the course of case proceedings based on facts and information that are submitted by litigants and lawyers, but also includes court's administrative and financial records, judicial statistics and secondary sources that make use of data generated by the courts."

[5] Chief Information Commissioner v. High Court of Gujarat., Civil appeal No(s). 1966-67 of 2020, para 24-25

FIGURE 1: WHAT IS JUDICIAL DATA UNIQUE?



B. WHAT KIND OF INFORMATION IS PRESENT IN JUDICIAL DATA THAT MAY IMPLICATE PRIVACY?

Court records contain a variety of information that can potentially impinge upon an individual's fundamental right to privacy. Given that "Courts are a stage where many of life's dramas are performed, where people may be shamed, vindicated, compensated, punished, judged, or exposed."[6] It is not surprising that court records and reporting of court proceedings, which serve as a chronicle of these events, are strewn with private and sensitive information. They contain personal information of the parties or litigants and witnesses, victims, law enforcement officials, etc., among other individuals who are drawn willingly or unwillingly into a legal dispute. For example, in suits for personal injury, medical malpractice, product liability, and so on, court files may contain vast quantities of data, such as medical history, mental health data, tax returns, and other financial information. Witnesses and other third parties involved in cases can have deeply personal details captured by discovery and later exposed in court documents. Information involved in money suits, tax matters and bankruptcy proceedings can contain personal identification numbers like Aadhar, PAN, bank account and card numbers, employment data, sources of income, expenses and debts. Family law matters can unmask the intimacies of marital relationships. In criminal cases, beyond the personal details about the victims, evidence presented by the accused person may contain information about their social history, character, family environment, education, employment and income.

In order to make judicial data more open and accessible without compromising other equally important considerations such as privacy, safety and security, it is essential to understand the nature of personal information that is processed by the courts and contained in its records and the degree of its sensitivity. The personal and sensitive personal data points found in court records can be broadly sorted into categories of information such as assets, education, employment, financial, identity, genetic and biometric, health, images, digital activity, location, sexual activity, intellectual pursuits, underscoring the privacy interests in such records. However, as privacy is often contextual, the list of categories is only indicative, and there may be other ways the individual information types can be categorised. Further, some data points may logically fit in multiple information categories.

Personal information arising in civil and criminal proceedings will often fall into a more specific category as listed above. Nevertheless, it is useful to organise data points separately under the head of civil and criminal proceedings to understand and contrast the kinds of sensitive information and the frequency with which they appear in the context of these two categories of cases. Civil proceedings capture types of information that relate to civil ....
For example, information about family and personal relationships (adoption, child support, guardianship, divorce, property disputes proceedings), information pertaining to health and medical history (accident and product liability cases), a person's disability or work performance (professional and employment proceedings, disciplinary actions) and prior adverse judgments etc. Individuals have no choice but to share these types of personal information in civil proceedings to make use of government services or remain law-abiding citizens. For criminal proceedings, on the other hand, the information types are associated with law enforcement and criminal judicial proceedings, including information that identifies an individual as the subject of a criminal investigation, arrest, incarceration, conviction, sentence, or parole. This category of information often includes mug shots,

[6] Amanda Conley, Anupam Datta, Helen Nissenbaum & Divya Sharma. 2011. 'Sustaining Privacy and Open Justice in the Transition to Online Court Records: A Multidisciplinary Inquiry,' Maryland Law Review, 71: 722

police investigation reports, sexual abuse allegations, search and seizure etc. Additionally, information about the victim, informant, witness, surety (in case of bail) also falls under this category. Forensic evidence like fingerprints, DNA as well as narco-analysis reports is also regarded as sensitive. For example, many scholars assert that the public disclosure of the names of crime victims and witnesses leads to the further victimisation of those who have suffered from or witnessed criminal activity. Others point to the stigma that is attached to individuals who have been subjected to criminal investigation, charge, or conviction. Even when acquitted, the information contained in criminal records may negatively affect an individual's social and professional life[7].

[7] David S. Ardia and Anne Klinefelter. 2015. 'Privacy and Court Records: An Empirical Study', Berkeley Technology Law Journal, 30(3): 1807-1898.

CHAPTER 3

WHAT MAKES JUDICIAL DATA UNIQUE?

The processes by which the judiciary adjudicates disputes is fundamental to its role. Its adherence to due process of law while doing so ensures a degree of fairness, consistency, and protection from arbitrariness[8]. The methods used by the judiciary to process the data that it obtains, the availability/ accessibility of data generated by the judicial process and the purposes for which such data is used should, therefore, be in consonance with the due process of law and with constitutional and other applicable principles. The following section discusses the unique doctrines, principles, and institutional arrangements that characterise the judicial process and the judiciary's relationship to information/data.

A. INDEPENDENCE OF THE JUDICIARY

The judiciary is independent of both the legislature and the executive. Judicial independence is therefore the pre-condition for the guarantee that all citizens will be treated equally by the courts. The power of courts to frame and enforce their own rules and their autonomy over decision making and the judicial process are critical to maintaining their independence. Therefore, independence of the judiciary extends not only to judicial functions (i.e. adjudicatory powers)[9] but to all actions carried out in a 'judicial capacity' (i.e. all functional capacities of a judge, whether administrative, adjudicatory or any other, necessary for the administration of justice)[10].

[8] AK Kraipak v. Union of India, AIR 1970 SC

[9] Reference Re Residential Tenancies Act, 123 DLR (3d) 554, Supreme Court of Canada cited with approval by the Supreme Court of India in Madras Bar Association v. Union of India, 2014 SCC Online SC 771

[10] Baradakanta Mishra v. The Registrar of Orissa High Court, 1974 SCR(2) 282

FIGURE 2: WHAT MAKES JUDICIAL DATA UNIQUE?

B. THE JUDICIAL PROCESS AND THE ROLE OF PARTICIPANTS

Academic literature has identified the following features that distinguish the judicial process from the legislative and/or administrative processes.

1. Traditionally, the judicial process is not initiated by the court on its own. It usually needs a claimant or a plaintiff (for example, a private party or the public prosecutor). "It is the fact that such application [of the person claiming rights] must be made to him, which distinguishes a judge from an administrative officer.[11]" In contrast, legislative and administrative processes can be initiated without waiting for an interested person's application.[12]

2. All the parties involved in a judicial proceeding must be given a fair opportunity to be heard by an impartial judge, either personally or through their representatives and the judge cannot have a personal interest in the case[13]. As a result, the vast quantities of data that the judiciary possesses are either the direct and voluntary contribution of the judicial participants or because of the need to comply with 'due process' requirements. In contrast, legislators and administrators can be deeply involved with a partisan interest in the matters they regulate. They can represent persons and groups and act in favour of them, without being obliged to listen to opposing interests and groups.[14]

3. Judicial decisions are expected to be based only on the information formally given to the system. Accordingly, judges are forbidden to discuss a case or to gather evidence outside the formal proceedings. In contrast, legislators and administrators (except when they are expected to perform in quasi-judicial capacity) may secure information whenever and however they please, contact rival claimants in private, and are under no obligation to listen to opposite interest groups or respond to their concerns.

C. OPEN COURTS

As a branch of government, the judiciary is subject to criticism, commentary and opinion expressed in the public sphere. However, courts and judicial officers have limited capacity to respond to public opinion due to the nature of the judicial role. Judicial engagement with the public is complicated by the fact that a court is not supposed to speak except through its judgments. While some audiences can be addressed directly (litigant, witness or attendees of the court as a member of the public, etc.), most people engage with the courts only indirectly or passively. Given these constraints on the judiciary's ability to communicate with the public, the open courts principle is the primary means of facilitating the interaction between the public and the judiciary.

[11] John C. Gray. 1909. Nature and Sources of the Law, 2nd edition 2019. New York City: Routledge.
[12] Mauro Cappelletti. 1989. The Judicial Process in Comparative Perspective. Oxford: Clarendon Press
[13] Neal Tate and Torbjorn Vallinder. 1995. The Global Expansion of Judicial Power. New York: New York University Press
[14] Cappelletti, The Judicial Process in Comparative Perspective

The practice of allowing public attendance in courts, referred to as holding trials in "open courts", is regarded as indispensable to the fair and proper administration of justice. Open courts requires that court proceedings be open to the public. At the core of this principle is the idea that the visibility of judicial proceedings serves as a check against abuse of authority and judicial excesses and is a means of ensuring that adjudication is a fair and consistent process. Not only is it integral to public confidence in the justice system, but it is also vital for the public's understanding of the administration of justice. Moreover, openness is a principal component of the legitimacy of the judicial process and why the parties to legal proceedings and the public at large abide by the decisions of courts.

> **"At the core of this principle (open courts) is the idea that visibility of judicial proceedings serves as a check against abuse of authority and judicial excesses and is a means of ensuring that adjudication is a fair and consistent process."**

In the Indian context, the Constitution states that the judgments of the Supreme Court of India shall be delivered only in open court[15]. Further, procedural law generally requires that all hearings in civil and criminal cases are held in full view of the public[16]. Section 153B of the Code of Civil Procedure (CPC), 1906 provides that the place of trial is generally an open court that it is to be accessible to the public, to the extent that it can accommodate them, unless the judge decides otherwise. It also provides that the evidence of the witnesses in attendance shall be taken orally in 'open court' in the presence and under the personal direction and superintendence of the judge.[17]. Similarly, section 327 of the Code of Criminal Procedure (CrPC) states that the place of inquiry or trial in criminal cases is to be an open court to the extent it can accommodate public attendance. Additionally, the evidence of witnesses should also be taken in an open court[18] and judgements should be pronounced in an open court[19].

Courts in India have also recognised open courts principle as integral to the rule of law. In *Naresh Sridhar Mirajkar v. State of Maharashtra*[20], the Supreme Court held that save in exceptional cases, the proceedings of a court of justice should be open to the public and that a public trial in open court is undoubtedly essential for the healthy, objective and fair administration of justice. More recently, in *Swapnil Tripathi v. Supreme Court of India*[21], the apex court while reiterating the importance of open courts, stated that, "the right of access to justice flowing from Article 21 of the Constitution or be it the concept of justice at the doorstep, would be meaningful only if the public gets access to the proceedings as it would unfold before the Courts and in particular, opportunity to witness live proceedings in respect of matters having an impact on the public at large or a section of people[22]." Further, it also held that the right to know and receive information is a facet of Article 19(1)(a) of the Constitution and for which reason the public is entitled to witness court proceedings involving issues having an impact on the public at large or a section of the public, as the case may be[23].

[15] Article 143(4) of the Constitution of India

[16] Section 153B, of the Code of Civil procedure (CPC), 1906 holds that the place of trial is to generally be an open court which is to be accessible to the public to the extent that it can accommodate them, unless the judge sees fit to revoke public access. As per section 327 of the Code of Criminal Procedure (CrPC), the place of inquiry or trial in criminal cases is to be an open court, to the extent it can accommodate public attendance. Judgment is to be pronounced in an open court under 265F. Additionally, the evidence of witnesses is to be taken in an open court under Sections 274, 275, and 276.

[17] Order 18, Rule 4 of the Code of Civil Procedure

[18] Sections 274, 275, and 276 of the Code of Criminal Procedure

[19] Section 265F of the Code of Criminal Procedure

[20] Naresh Shridhar Mirajkar v. State of Maharashtra, (1966) SCR (3) 744

[21] Swapnil Tripathi v. Supreme Court of India, (2018) 10 SCC 628

[22] Swapnil Tripathi v. Supreme Court of India, (2018) 10 SCC 628, paragraph 2

[23] Swapnil Tripathi v. Supreme Court of India, (2018) 10 SCC 628, paragraph 3

LIMITATIONS ON OPEN COURTS

Open courts is the general rule. However, the rule is not absolute. It is necessary to consider the exceptions that this rule permits. In *Naresh Sridhar Mirajkar v. State of Maharashtra*[24], the Supreme Court observed, "administration of justice is the primary object of the work done in courts; and so, if there is a conflict between the claims of administration of justice itself and those of public trial, a public trial must yield to the administration of justice." It held that the High Courts have inherent jurisdiction to hold a trial in camera if the ends of justice clearly and necessarily require the adoption of such a course. However, this inherent power must be exercised with great caution only if the court is satisfied beyond doubt that the ends of justice themselves would be defeated if a case is tried in open court. Further, such power includes the power to hold a part of the trial in-camera or to prohibit excessive publication of a part of the trial[25]. The Court relied on the celebrated decision of the House of Lords in Scott v. Scott where it was held that courts of justice have no power to hear cases in-camera even by consent of the parties, except in exceptional cases in which a hearing in open court might defeat the ends of justice. Similarly, in *Kehar Singh v. State (Delhi Administration)*[26] , the Court upheld the holding of trial in the jail while emphasising that even though public trial or trial in open court is the rule, yet in cases where the ends of justice would be defeated if the trial is held in public, the court has inherent jurisdiction to hold a trial in-camera. More recently, in *Swapnil Tripathi v. Supreme Court of India*, the Court, while applying the underlying principle that administration of justice itself may make it necessary for the courts to hold in-camera trials, held that it might be appropriate to have a proper and balanced regulatory framework before the concept of live streaming of court proceedings is put into action[27]. Such a framework should be mindful of the various interests regarding the administration of justice, including open justice, dignity and privacy of the participants to the proceedings and the majesty and decorum of the courts[28]. Therefore, while the general rule is well settled that court proceedings (civil or criminal) be open to the public, in exceptional circumstances, the fair and proper administration of justice may justify a deviation from the principle of open courts.

At this juncture, it will be useful helpful to emphasise that the judiciary and the judicial process have a set of characteristics that must be considered before embarking on any discussion on a privacy and data protection framework for it. Privacy and data protection principles should not be viewed as changing the balance or diminishing the value of fairness inherent in the justice system. In other words, such principles themselves should not create an advantage or a disadvantage to any part of the justice system or serve to "close" the system to the public.

[24] Naresh Shridhar Mirajkar v. State of Maharashtra, (1966) SCR (3) 744
[25] Naresh Shridhar Mirajkar v. State of Maharashtra, (1966) SCR (3) 744
[26] Kehar Singh v. State (Delhi Administration), 1988 AIR 1883
[27] Swapnil Tripathi v. Supreme Court of India, (2018) 10 SCC 628, paragraph 7
[28] Swapnil Tripathi v. Supreme Court of India, (2018) 10 SCC 628, paragraph 18

CHAPTER 4

COURT RECORDS IN THE DIGITAL ENVIRONMENT AND IMPLICATIONS ON PRIVACY

A. TECHNOLOGY AND OPEN COURTS

Technology can enhance public access, ensure transparency and pave the way for active citizen involvement in the functioning of state institutions. The interplay between technology and law has allowed the dissemination of legal information with a veritable click of a button. There is now an expectation that technology will be leveraged to boost the principles of open justice. The judiciary must find a way to meet these expectations whilst preserving the fundamental aspects of the rule of law - fairness and judicial impartiality.

The Indian judiciary has incorporated Information and Communication Technology (ICT) under the e-Courts Integrated Mission Mode Project (e-Courts Project). While Phase-I enabled the computerisation of courts across the country, Phase-II concentrated on enhancing service delivery for litigants and lawyers by improving infrastructure and providing technology-enabled judicial processes (e-filing, e-payment). It involved improved ICT infrastructure, videoconferencing, improved access across seven platforms, including a web portal, app, judicial service centres and kiosks. Courts across India, both in the higher and district judiciary and tribunals, are moving quickly to digitise their records and make them available online. The National Judicial Data Grid, a public access portal provides national, state, district and court-wise information about institution and disposal of cases. Further, in a landmark judgement in 2018, the Supreme Court laid down guidelines for live-streaming of court proceedings, following which several courts have begun doing so.

All these efforts have had two primary effects on open courts: wider dissemination of information and easier access to information. A large segment of society can rarely can attend court proceedings due to constraints like poverty, distance, time, cost and resources. Video-conferencing and live-streaming provide a cost-effective and efficient alternative to access court proceedings. In light of the growing internet penetration in the country, it is most suited for connecting geographically dispersed audiences. This makes direct dissemination of information possible to a wider audience who would generally have not been able to attend court proceedings and had to rely on second-hand information provided by the lawyers (to their clients) and the media (to the members of the public). Technology has also made it easier to search, inspect and analyse judicial information.

> **Practical obscurity refers to the idea that publicly available information can still have private attributes if it is difficult to access, find, or contextualise**

B. HOW IS ONLINE ACCESS TO COURT RECORDS DIFFERENT FROM TRADITIONAL PAPER-BASED RECORDS?

The increasing use of information technology in the justice system and rapid technological advancements have transfromed how court information is structured, captured, stored, accessed, maintained, distributed, secured and preserved. Implementing innovative technology applications will help the judiciary to meet the changing needs of the judiciary and the public. However, the adoption of technology also warrants re-thinking the traditional information management policies and practices of the judiciary that are intrinsically based on a paper paradigm. The formulation of new, effective policies, therefore, requires us to account for the differences between physical access to the traditional paper-based records versus remote/online access to digitised and electronic court records. Some of the important differences are discussed below.

1. PRACTICAL OBSCURITY

"Practical obscurity" refers to the idea that publicly available information can still have private attributes if it is difficult to access, find, or contextualise[29]. Paper records, by their nature, provide "practical obscurity" of the information contained within them because anyone who wishes to peruse a court file has to travel to the paper file's physical location to access it. This presented a natural barrier to access because it required investment of time and money - enough to ensure that it was unlikely that such information would be widely disseminated in the absence of independent interest in the proceedings. Electronic information or digitised records, on the other hand, may be easily disseminated via the internet anywhere and anytime at a very low cost therefore making it easily accessible to the world at large[30].

[29] Woodrow Hartzog and Frederic Stutzman, The Case for Online Obscurity, 101 California Law Review 1, 21 (2013)

[30] Jo Sherman, Court Information Management – Policy Framework to Accommodate the Digital environment, 2013, Canadian Judicial Council, available online at: https://cjc-ccm.ca/sites/default/files/documents/2019/Policy%20Framework%20to%20Accommodate%20the%20Digital%20Environment%202013-03.pdf (last accessed on June 2 2021).

2. DOCUMENT 'VERSUS' INFORMATION'

Whereas a traditional court file comprised several documents, a modern court file will contain a large number of information fields that may be sourced from and dispersed across a variety of different locations. It is more granular because it needs to be considered in terms of the many separate components of information that reside within it. Electronic copies of the file or components within it may reside in multiple replicated locations within and outside the court. The notion of control over the file is much more difficult to translate into the digital domain due to this fragmentation, distribution and duplication of information. Further, complexity arises from the fact that court files nowadays comprise a collection of distinct information components or fields of data that are held in case management database systems rather than in documents on a paper file. It is now possible to manage and exchange 'fields of information' rather than capturing the information within paper 'documents'. The situation described above is not yet the norm in Indian courts. However, with steady progress being made in e-filing and smart form-based filings, this could soon become the reality. For this reason, court rules, practice directives and policies on the management of court information need to focus increasingly on information fields rather than on documents.[31]

3. POSSESSION AND CONTROL

Developing policy and implementing technology for the ownership and control of court information is far more complex in the digital domain than it was in a paper-based world. In a traditional court environment, the 'official court record' is generally held in paper files located in courthouses under the physical control of the judiciary. In a paper-based world, possession of a court file is synonymous with control over that file. Since an original court file could only reside in one physical location at a time, those with possession of the physical file could easily control access to the information within it. In the digital domain, however, it is quite possible to have possession of information without control and conversely, it is possible to have control of information without physical possession. Therefore, the concept of control in relation to electronic court records needs to move away from traditional notions linked to physical possession. Locating a server within a courthouse will not necessarily deliver control over its contents to the judiciary who work within that building. Conversely, if appropriate governance arrangements and safeguards are established, exercising control over court information residing in remote hardware may be possible[32].

[31] Jo Sherman, Court Information Management – Policy Framework to Accommodate the Digital environment, 2013, Canadian Judicial Council, available online at: https://cjc-ccm.ca/sites/default/files/documents/2019/Policy%20Framework%20to%20Accommodate%20the%20Digital%20Environment%202013-03.pdf (last accessed on June 2 2021).

[32] Jo Sherman, Court Information Management – Policy Framework to Accommodate the Digital environment, 2013, Canadian Judicial Council, available online at: https://cjc-ccm.ca/sites/default/files/documents/2019/Policy%20Framework%20to%20Accommodate%20the%20Digital%20Environment%202013-03.pdf (last accessed on June 2 2021).

C. IMPLICATIONS ON PRIVACY

1. LOSS OF OBSCURITY

One of the longstanding conceptions of privacy involves secrecy and it is lost once information is disclosed. Legal and privacy scholar Daniel Solove refers to this as the "secrecy paradigm". Using this paradigm, an invasion of privacy consists of "concealed information" being unveiled or released in some way to others. Another central form of invasion is being watched or listened to. Further, he states that privacy is often understood as an exclusive status or domain. Information is categorised as either public or private. When information is private, it is hidden, and as long as it is kept secret, it remains private. On the other hand, when information is public, it is in the public domain available for any use, and a person can no longer claim that the information is private. Understood this way, information can either be in one domain or another. The law often treats information in this black-and-white manner; either it is wholly private or wholly public. He then goes on to critique this paradigm in the information age as outmoded, and warns that it could lead to the practical extinction of privacy. He argues that privacy involves an expectation of a certain degree of accessibility of information. Under this alternative view, privacy entails control over and limitations on certain uses of information, even if the information is not concealed (or secret). Privacy can be violated by altering levels of accessibility, by taking obscure facts and making them widely accessible.[33] We expect that our lives will remain private because our personal information is a needle in a haystack, that will be lost in a sea of information, and usually nobody will take the time to try to find it. However, this anonymity is rapidly disappearing as access to information is increasing.

In *United States Department of Justice v. Reporters Committee for Freedom of the Press*, the United States Supreme Court held that the release of FBI rap sheets (containing information like date of birth, physical description, and a history of arrests, charges, and convictions of over twenty-four million people in the United States) would constitute an invasion of privacy. The court rejected the reporters' argument that the events summarised in the rap sheet were not private because they had previously been publicly disclosed. The Court observed:

"In an organized society, there are few facts that are not at one time or another divulged to another. Thus, the extent of the protection accorded a privacy right at common law rested in part on the degree of dissemination of the allegedly private fact and the extent to which the passage of time rendered it private. . . Recognition of this attribute of a privacy interest supports the distinction, in terms of personal privacy, between scattered disclosure of the bits of information contained in a rap sheet and revelation of the rap sheet as a whole...there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerised summary located in a single clearinghouse of information.34"

[33] Daniel J. Solove, Access and Aggregation: Privacy, Public Records, and the Constitution, 86 Minn. L. Rev. 1137 (2002)

[34] United States Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749,762–64 (1989)

In the paper-based world of court records, one had to know the case number in order to access a court record at the clerk's office. With electronic court records, the information in a court's files can be searched, sorted, and combined with other information without any need to maintain the record's connection to a specific case. This allows court records to be analysed and used along lines and from vantage points that were previously blocked.

2. EFFECT OF PASSAGE OF TIME

Paper records also exist temporally in a different way from electronic records. Over time, physical records accumulate and grow old and must be cleared away to make room for the new records. Paper records move from active case files, to closed case files, and eventually to long-term storage or destruction. The lifecycle for a paper court record therefore involves increasing levels of obscurity. On the other hand, electronic records continue to exist, potentially forever and unlike paper records, are rarely subject to the temporal degradation in access. As a result, records from cases that conclude today will remain just as accessible a decade from now. The passage of time may actually increase the privacy interest at stake when disclosure would revive the information that was once public knowledge but has long since faded from memory. This is especially relevant in the context of the 'right to be forgotten'.

FIGURE 3: COURT RECORDS IN THE DIGITAL ENVIRONMENT

PHYSICAL RECORDS

Practical Obscurity
Physical Records exist in 'practical obscurity' meaning access is technically allowed, but getting them is complex, expensive, or time consuming

'Document' vs. 'Information'
Case files are composed of documents, with manual effort needed to extract information, and it must be obtained from a single location

'Possession' vs. 'Control'
For physical court files, the originals are retained by the court, and possession of the documents enables controlling access.

DIGITAL RECORDS

Remote access
Digital access entails the removal of practical obscurity, enabling quick, cheap, remote access to large quantities of records

Move towards 'information'
Specific 'fields' of information can be extracted and combined from digital records across multiple locations

Lack of control
In the digital context, mere possession of data does not guarantee control of access to such data as there is no physical possession of a tangible document

IMPLICATIONS

Loss of obscurity
information which people would expect to be private can now be accessed easily, enabling invasions of privacy

Effect of time
Paper documents have a finite lifecycle, but digital information does not degrade, and becomes increasingly cheaper to store.

Aggregation
The ability to easily access and combine digital information enables insights about a person that are difficult when one has access to the same information, but from distinct physical sources

RISKS

Information on the internet cannot be controlled

Use of judicial data out of context compromises data accuracy and quality

Data mining enables unauthorised bulk access to judicial data for commercial gain

Unlimited access to judicial may increase personal safety risks for vulnerable people.

Privacy may be invaded by persons with no right to know

Increased risk of identity theft, harassment, fraud

Lack of privacy may deter people from going to court

3. AGGREGATION

Another longstanding notion of privacy is that it protects against the disclosure of sensitive or intimate information. According to this view, information that we should protect as private must be embarrassing or harmful to one's reputation. Some argue that the information in public records, including court records, consists of fairly innocuous details such as one's name, birth date, address, and so on which are not ordinarily personal, intimate, or embarrassing pieces of information and thus do not pose immediate harm to one's reputation or security. However, this only holds true when each piece of information is viewed in isolation. Viewed in combination, these pieces of information begin to paint a portrait about our personalities referred to as the "aggregation problem". The aggregation problem arises because the digital revolution has enabled information to be easily amassed and combined to create a "digital biography" about individuals. In the digital world, information breeds information. Even seemingly innocuous and incomplete information about a person contained in public records can be quite useful in obtaining more data about such individuals.

Further, public records, including court records, are often a principal source of information for the private sector in constructing their databases. Marketers stock their databases with public record information, and the uses to which these databases are put are manifold and potentially limitless. The problem is that often without the individual's knowledge or consent, the information is then used for a host of different purposes[35].

D. POTENTIAL RISKS AND CONSEQUENCES

In an increasingly networked and digitised society, many new challenges and risks may be encountered which were not present in the paper-based world. Some of these risks are discussed below.

1. **It is impossible to control information once it's released on the internet.** Once electronic court information has been released, particularly via the internet, it can potentially be accessed, aggregated, collated, mined, repackaged, disseminated and commercialised by persons or organisations with no authority to do so.

2. **Quality and accuracy of information are compromised through de-contextual use of the information contained in court filings and court decisions**. If information about individuals is extracted from court filings and exploited through data mining or combined with additional information acquired from other sources, the original context is lost. This can lead to the development of behaviour profiles of individuals, stereotyping, and to decisions based on "secretive data processing" because the processing is hidden from the individuals. In effect, by making all this information about the citizen so transparent, the public does not really know what happens to their personal information and, ironically, the accuracy of the information describing individuals can be compromised through out-of-context compilations and profiling[36].

[35] Daniel J. Solove, "Access and Aggregation: Privacy, Public Records, and the Constitution" (2002) 86 Minn. L. Rev. 1137

[36] Reena Raggi, Daniel J. Capra, Joel Reidenberg, and Ronald Hedges, "Panel One: General Discussion on Privacy and Public Access to Court Files" (2011) 79 Fordham L. Rev. 1 pg 5

3. **Data mining may facilitate unauthorised bulk access to court information which can be re-packaged and distributed for commercial gain**. There is a widespread understanding that electronic access should not facilitate bulk searches or problematic data mining of personal information found in court records for commercial purposes[37]. Bulk access, when permitted, must be accompanied by adequate safeguarsd and oversight mechanisms like audits, inspections etc.

4. **Unlimited access to online court information may increase personal safety risks for vulnerable people.** This is particularly a concern in criminal and family law cases and cases involving juvenile justice. If this consideration is not accommodated in systems that deliver court information online, the risks can be more significant than they were in the traditional paper-based world due to the ease with which anyone with internet access can access the information. Further, criminal records and other sensitive records relating to vulnerable people can get inappropriately distributed and accessible in an integrated justice information system programs where there is a loss of control as data flows downstream from courts into other agencies. The mitigation of such risks needs to be built into the architecture of such systems.[38].

5. **Privacy may be invaded by persons with no right to know.** Broad, unrestricted access to court information can facilitate 'busybody' enquiries and privacy violations due to the removal of practical obscurity barriers prevalent in a physical world.

6. **Increased risk of identity theft, harassment, fraud.** Broad access to court information without adequate protection of personal information may facilitate identity theft and fraud where personal details are inadvertently or purposefully embedded within the accessible information[39]. Unregulated access to court record online could add to the problems of witness coercion and facilitate an intimidation industry[40]. Data mining can begin with litigants, witnesses, or statements made in a court filing and expand to the judges and their personal lives[41].

7. **The ease with which court information can potentially be accessed online by the media or general public may deter litigants from pursuing resolution of their disputes through the court system.** Traditionally, judicial participants have disclosed personal and sensitive information with the understanding it would be used only to resolve the dispute in the context of the judicial process. If the personal cost for engaging with the legal system is a perceived loss of privacy because the data is now publicly accessible, freely searchable on the web, the public may hesitate to participate in the judicial system[42].

[37] Lisa M. Austin and Frédéric Pelletier, Synthesis of the Comments on Judges Technology Advisory Committee Discussion Paper on Open Courts, Electronic Access to Court Records, and Privacy prepared for the Canadian Judicial Council, January 2005, para 55-57, available online at: https://cjc-ccm.ca/sites/default/files/documents/2019/news_pub_techissues_Synthesis_2005_en.pdf (last accessed on June 2 2021).

[38] Jo Sherman, Court Information Management – Policy Framework to Accommodate the Digital environment, 2013, Canadian Judicial Council, available online at: https://cjc-ccm.ca/sites/default/files/documents/2019/Policy%20Framework%20to%20Accommodate%20the%20Digital%20Environment%202013-03.pdf (last accessed on June 2 2021).

[39] In one United States case, seven co-conspirators used personal information obtained from court records available on PACER to open false financial accounts. Around 34 inmates and 20 financial institutions were victimized. In another instance, a speeding ticket posted on a court clerk's website provided an identity thief with a person's social security number, address, height, weight, birth date and his signature. The thief accumulated $11,000 in credit card theft before his arrest. See Lynn Eicher Sudbeck, "Placing Court Records Online: Balancing Judicial Accountability with Public Trust and Confidence – An Analysis of State Court Electronic Access Policies And a proposal for South Dakota Court Records" (2005). Institute for Court Management, Court Executive Development Program Phase -III, State Court Administrator's Office South Dakota Unified Judicial System Pierre, South Dakota, available online at: https://www.ncsc.org/__data/assets/pdf_file/0017/16811/sudbecklynncedpfinal32905.pdf (last accessed on 2 June 2021)

[40] David L Snyder, "Nonparty Remote Electronic Access to Plea Agreements in the Second Circuit" (2008) 35:5 Fordham Urb LJ 1263

[41] In 2016, a lawyer and machine learning expert, Michaël Benesty, published an analysis of French asylum decisions which showed that some judges rejected almost all asylum requests while others had a very low ratio of rejection. Benesty created a website where members of the public could observe ongoing variation amongst the judiciary on asylum cases and use the software to analyse judicial bias in other types of decisions. As a result, in 2019, France passed a law criminalizing certain types of analytics of judges' decisions, to limit 'forum-shopping' by litigants. See Malcolm Langford and Mikael Rask Madsen, "France Criminalises Research on Judges" (2019) Verfassungsblog on Matters Constitutional, available online at: https://verfassungsblog.de/france-criminalises-research-on-judges/#:~:text=In%20March%2C%20France%20made%20a,remarkable%20five%20years%20in%20prison. (last accessed on 2 June 2021)

[42] Reena Raggi, Daniel J. Capra, Joel Reidenberg, and Ronald Hedges, "Panel One: General Discussion on Privacy and Public Access to Court Files" (2011) 79 Fordham L. Rev. 1 pg 5

In conclusion, the "practical obscurity" fostered by paper-based records ensured a close connection between the purposes for seeking access to court records and the rationale behind open courts principle. The move towards an electronic environment challenges the connection between the purpose of access and the purpose of open courts. Furthermore, the electronic environment permits the linking and aggregation of personal information, heightening the privacy interest of individuals in controlling that information. The move towards electronic access, therefore, raises the possibility that such access might facilitate some uses of information that are not firmly connected to the underlying rationale for the right to open courts and which might have a significant negative impact on values such as privacy or the administration of justice more generally[43].

[43] Lisa M. Austin and Frédéric Pelletier, Synthesis of the Comments on Judges Technology Advisory Committee Discussion Paper on Open Courts, Electronic Access to Court Records, and Privacy prepared for the Canadian Judicial Council, January 2005, available online at: https://cjc-ccm.ca/sites/default/files/documents/2019/news_pub_techissues_Synthesis_2005_en.pdf (last accessed on June 2 2021).

CHAPTER 5

PRIVACY UNDER INDIAN LAW

A. PRIVACY AS A FUNDAMENTAL RIGHT

In 2017, the Supreme Court of India in *K.S. Puttuswamy v. Union of India*[44] *(hereinafter Puttuswamy I)* declared that the right to privacy is a fundamental right that is protected as an intrinsic part of the right to life and personal liberty under Article 21[45]. Privacy is the necessary condition precedent to the enjoyment of any guarantees in Part III (fundamental rights) of the Constitution. As a result, a right to privacy may be situated not only in Article 21 but also simultaneously in any of the other guarantees in Part III[46]. The right to privacy is inextricably bound up with all exercises of human liberty – both as it is enumerated explicitly across Part III and as it is guaranteed in the residue under Article 21. It is distributed across the various articles in Part III and, mutatis mutandis, takes the form of whichever of their enjoyment its violation curtails[47]. The fundamental right of privacy, which has so many developing facets, can only be developed on a case-to-case basis. Depending upon the particular facet that is relied upon, either Article 21 by itself or in conjunction with other fundamental rights would get attracted[48].

[44] K.S. Puttuswamy v. Union of India, 2017 10 SCC 1 decided on 24 August 24 2017 (hereinafter referred to as Puttuswamy I)
[45] Puttuswamy I, Order of the Court, para 2(iii)
[46] Puttuswamy I, Justice S.A. Bobde, para34
[47] Puttuswamy I, Justice S.A. Bobde, para 47
[48] Puttuswamy I, Justice R.F. Nariman, para 85

FIGURE 4: CURRENT LEGAL STATUS OF PRIVACY

The **Puttuswamy I** judgment recognised privacy as a fundamental right under Part III of the Constitution of India, particularly Articles 14, 19, and 21

The **Puttuswamy II** judgment defined the contours of privacy further

Whether a restriction of the right to privacy, is constitutional depends on which corresponding fundamental right is curtailed by state action

Under Article 14, the state action has to be tested on the grounds of 'manifest arbitrariness'

Grounds mentioned under Article 19 include the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence

Under Article 21, the state action must meet the requirements of (i) legality, which postulates the existence of law; (ii) need, defined in terms of a legitimate state aim/interest; and (iii) proportionality, which ensures a rational nexus between the objects and the means adopted to achieve them

The court accepted the following test for proportionality:
A measure restricting a right
(i) Must have a legitimate goal
(ii) It must be a suitable means of furthering this goal
(iii)There must not be any less restrictive but equally effective alternative
(iv)The measure must not have a disproportionate impact on the right holder

It is a concomitant of the right of the individual to exercise control over his or her personality

It is necessary condition precedent to the enjoyment of any of the guarantees in Part III

It covers intrusion with an individual's physical body, informational privacy, and privacy of choice.

Privacy is intrinsic to freedom, liberty and dignity. The sanctity of privacy lies in its relationship with dignity.

It has both positive and negative content

Right to privacy cannot be impinged without a just, fair and reasonable law

Justice S.A. Bobde explains the interrelationship between Article 21 and other fundamental rights in Part III in the following manner:

"There is no doubt that privacy is integral to the several fundamental rights recognised by Part III of the Constitution and must be regarded as a fundamental right itself. The relationship between the right of privacy and the particular fundamental right (or rights) involved would depend on the action forbidden by a particular law. At a minimum, since privacy is always integrated with personal liberty, the constitutionality of the law which is alleged to have invaded into a rights bearer's privacy must be tested by the same standards by which a law that invades personal liberty under Article 21 is liable to be tested...Once it is established that privacy imbues every constitutional freedom with its efficacy and that it can be located in each of them, it must follow that interference with it by the state must be tested against whichever one or more Part III guarantees whose enjoyment is curtailed. As a result, privacy violations will usually have to answer to tests in addition to the one applicable to Article 21[49]..."

Therefore, the right to privacy as a fundamental right is not limited to Article 21. On the contrary, privacy resonates through the entirety of Part III of the Constitution which pertains to fundamental rights and, in particular, Articles 14, 19 and 21[50].

[49] Puttuswamy I, Justice S.A. Bobde, paras 45 and 46

[50] K.S. Puttuswamy v. Union of India, (2019) 1 SCC 1, decided on 26 September 2018 (hereinafter referred to as Puttuswamy II), para 84

B. CONTOURS AND SCOPE OF RIGHT TO PRIVACY

While deciding the constitutionality of Aadhaar Act, the Supreme Court of India in 2018 in *K.S. Puttuswamy v. Union of India*[51] (hereinafter Puttuswamy II) summarised the contours of right to privacy as stated below[52]:

(i) Privacy has always been a natural right.

It is a concomitant of the right of the individual to exercise control over his or her personality

It is the necessary condition precedent to the enjoyment of any of the guarantees in Part III

It covers at least three aspects – (i) intrusion with an individual's physical body, (ii) informational privacy, and (iii) privacy of choice.

One aspect of privacy is the right to control the dissemination of personal information. Every individual should have a right to be able to control exercise over his/her own life and image as portrayed in the world and to control commercial use of his/her identity

(ii) The sanctity of privacy lies in its functional relationship with dignity.

(iii) Privacy is intrinsic to freedom, liberty and dignity

(iv) Privacy has both positive and negative content

(v) Informational privacy is a facet of right to privacy

(vi) Right to privacy cannot be impinged without a just, fair and reasonable law

Further, the Court discussed three approaches to formulating privacy[53]. Privacy can be classified on the basis of harms[54], interests[55] and as an aggregation of rights[56][57]. The Court cautioned that future developments in technology and social ordering may reveal that there are yet more constitutional sites in which a privacy right inheres that are not evident at present[58].

[53] Puttuswamy II, para 85; See the analysis of Puttuswamy I by the Centre for Internet and Society, https://cis- india.org/internet-governance/blog/the-fundamental-right-to-privacy-an-analysis

[54] Daniel Solove, Understanding Privacy, Cambridge, Massachusetts: Harvard University Press, 2008.

[55] This taxonomy deals with the sub-areas within the right to privacy protect different 'interests' or 'justifications'. According to the Court, Justice J. Chelameswar's adopted this approach to privacy in Puttuswamy I when observing that privacy includes the three interests - privacy of repose, privacy of sanctuary and privacy of intimate decision.

[56] This approach in classifying privacy as a right is not limited to one particular provision in the Chapter of Fundamental Rights under the Constitution but is associated with amalgam of different but connected rights.

[57] Puttuswamy I, Justice R.F. Nariman para 85, Justice S.A. Bobde para 41

[58] Puttuswamy I, Justice S.A. Bobde para 34

C. LIMITATIONS ON THE RIGHT TO PRIVACY

Like other rights which form part of the fundamental freedoms protected by Part III, privacy is not an absolute right. A law which encroaches upon privacy will have to withstand the touchstone of permissible restrictions on fundamental rights[59].

The circumstances under which the right to privacy may be limited by state action have to be examined from the point of view of Articles 14, 19 and 21 since the right to privacy has an intimate connection to various rights in Part III and is not only related to Article 21.. Therefore, any interference with privacy by the State must satisfy the tests applicable to whichever one or more of the Part III freedoms the interference affects[60]. One must keep in mind that at a minimum, since privacy is always integrated with personal liberty (guaranteed under Article 21), any curtailment of privacy is always liable to be tested against the standards under Article 21. Depending on the nature of interference, privacy violations will also have to answer tests under various provisions of Part III (including Articles 14 and 19) in addition to the test under Article 21[61].

Under **Article 14**, the state action has to be tested on the grounds of **'manifest arbitrariness'**.

When it comes to examining the 'restrictions' as per the provisions of Article 19, such restriction must satisfy:

(i) **Grounds mentioned under Article 19(2) to Article 19(6**) depending on the particular freedom that has been restricted under Article 19(1). Such grounds include (i) the sovereignty and integrity of India, (ii) the security of the State, (iii) friendly relations with foreign States, (iv) public order, (v) decency or morality or (vi) in relation to contempt of court, (vii) defamation or (viii) incitement to an offence; and

(ii) **Restriction should be reasonable.** Courts have applied multiple standards to determine reasonableness, including proximity, arbitrariness, and proportionality.

In the context of **Article 21** an invasion of privacy must be justified on the basis of a law which stipulates a procedure which is fair, just and reasonable. The law must also be valid with reference to the encroachment on life and personal liberty under Article 21. According to Puttuswamy I (and later adopted by Puttuswamy II), an invasion of life or personal liberty must meet the three-fold requirement[62] of:

(i) Legality, which postulates the **existence of law**; There must be a law in existence to justify an encroachment on privacy since no person can be deprived of his life or personal liberty except in accordance with the procedure established by law[63].

(ii) Need, defined in terms of a **legitimate state aim/interest[64];**
The requirement of a need, in terms of a legitimate state aim, ensures that the nature and content of the law which imposes the restriction falls within the zone of reasonableness mandated by Article 14, which is a guarantee against arbitrary state action[65].

(iii) **Proportionality**, which ensures a rational nexus between the objects and the means adopted to achieve them.

[59] Puttuswamy I, Justice D.Y. Chandrachud for himself and Justice Jagdish Chandra Kehar, Justice R.K. Agrawal and Justice S. Abdul Nazeer, Part T, para 3(H)

[60] Puttuswamy II, para 87

[61] Puttuswamy I, Justice S.A. Bobde para 47 c.

[62] Puttuswamy I, Justice D.Y. Chandrachud for himself and Justice Jagdish Chandra Kehar, Justice R.K. Agrawal and Justice S. Abdul Nazeer, Part T, para 3(H); Puttuswamy II, para 117

[63] Article 21, Constitution of India

[64] In Puttuswamy II, the Court noted that different judges proposed slightly differing standards of review. While Justice D.Y. Chandrachud formulated the test of 'legitimate state interest', two of the Judges, namely, Justice J. Chelameswar and Justice A. M. Sapre proposed the test of 'compelling state interest', Justice S.K. Kaul adopted the test of 'public interest'. Further, Justice R.F. Nariman pointed out that the Right to Information Act, 2005 has provided for personal information being disclosed to third parties subject to 'larger public interest' being satisfied. If this test is applied, the result is that one would be entitled to invoke 'large public interest'. Puttuswamy II than concluded that since judgment of Justice D.Y. Chandrachud was on behalf of himself and three other Judges and Justice S.K. Kaul also virtually adopted the same test, the majority opinion endorsed the test of 'legitimate state interest' as the standard for review.

[65] Puttuswamy I, Justice D.Y. Chandrachud for himself and Justice Jagdish Chandra Kehar, Justice R.K. Agrawal and Justice S. Abdul Nazeer, Part T, para 180

This requirement ensures that the means adopted by the legislature are proportional to the object and needs sought to be fulfilled by the law. Proportionality is an essential facet of the guarantee against arbitrary state action because it ensures that the nature and quality of the encroachment on the right is not disproportionate to the purpose of the law[66].

The Supreme Court in Puttuswamy II explained the doctrine of proportionality. In order to ascertain the proportionality of the state action curtailing privacy to the object sought to be achieved, it adopted the test laid down in *Modern Dental College and Research Centre & Ors. v. State of Madhya Pradesh & Ors*[67]. There are four sub-components of proportionality that need to be satisfied for a limitation on a constitutional right to be permissible. These are:

(i) A measure restricting a right must have a legitimate goal (legitimate goal stage)

(ii) It must be a suitable means of furthering this goal (suitability or rationale connection stage)

(iii) There must not be any less restrictive but equally effective alternative (necessity stage)

(iv) The measure must not have a disproportionate impact on the right holder (balancing stage)

In addition to the four sub-components listed above, Puttuswamy II also endorsed the steps suggested by Professor David Bilchitz[68] that help in determining proportionality. The steps include[69]:

(i) Firstly, identifying a range of possible alternatives to the measure employed by the government

(ii) Secondly, determining the effectiveness of these measures individually to ascertain whether each respective measure realises the governmental objective in a 'real and substantial manner' (and not whether the measure realises the governmental objective to the same extent)

(iii) Thirdly, determining the impact of the respective measures on the right at stake

(iv) And lastly, an overall judgment as to whether in light of the findings of the previous steps, there exists a preferable alternative.

[66] Puttuswamy I, Justice D.Y. Chandrachud for himself and Justice Jagdish Chandra Kehar, Justice R.K. Agrawal and Justice S. Abdul Nazeer, Part T, para 180

[67] Puttuswamy II, para 126

[68] David Bilchitz ,'Necessity and Proportionality: Towards A Balanced Approach?', Hart Publishing, Oxford and Portland, Oregon, 2016.

[69] Puttuswamy II, para 123

D. RIGHT TO DATA PROTECTION

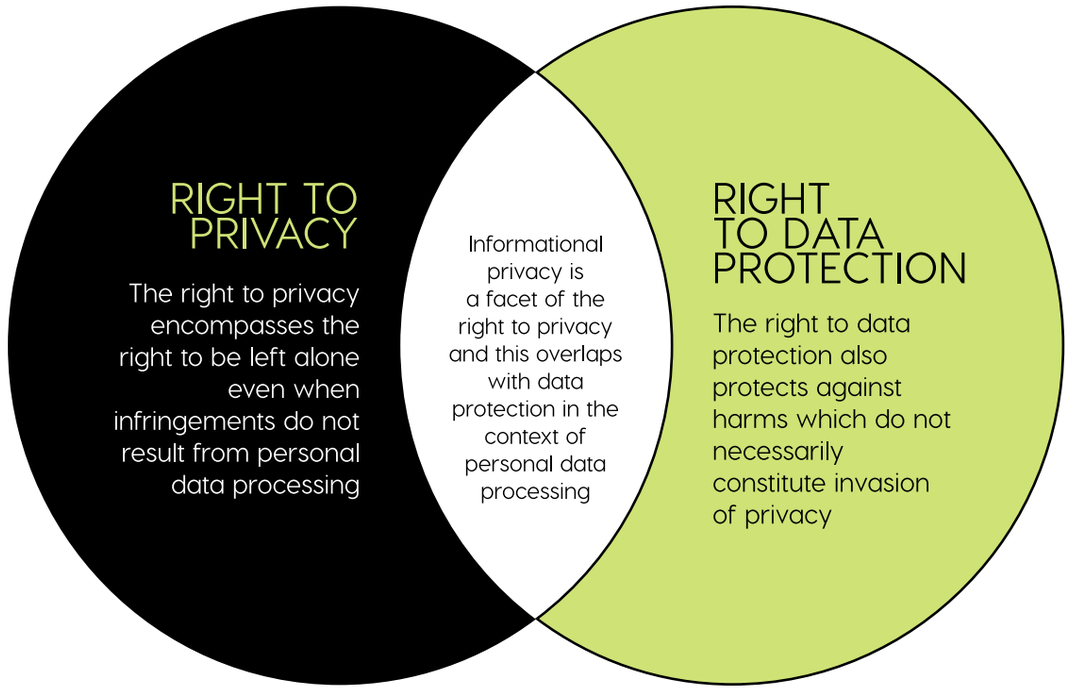
Is the right to data protection an expression of the right to privacy, or is it completely distinct? Firstly, it is the mere processing of personal data that allows data subjects to invoke their rights based on the right to data protection, irrespective of whether their right to privacy has been infringed or not. The Court of Justice of European Union has held that "(...) the mere recording by an employer of data by name relating to the remuneration paid to his employees cannot as such constitute an interference with private life". According to the Court, the recording of personal data, by itself, thus did not fall within the scope of the right to privacy, whereas the Court noted that such a recording falls within the scope of the right to data protection since it constitutes personal data processing[70]. The individual rights based on the right to privacy are, therefore, of a more context-sensitive nature. Accordingly, the protection offered by the right to privacy and the right to data protection also differs. For example, the right to privacy as a fundamental right can only be enforced against the state, while the right to data protection also applies horizontally (and not only towards the state). The aim of data protection is to regulate a specific practice, namely, the processing of personal data. Hence, a data protection regime by default accepts the processing of personal data; otherwise, its aim would be void. Such a regime establishes safeguards and thresholds geared towards protecting the individual's liberty when data about him/her are processed[71]. It is in this sense that data protection is a legal mechanism that ensures privacy.

> "... Personal data protection and privacy overlap on a mode whereby data protection is both broader and narrower than privacy. It is narrower because it only deals with processing personal data, whereas the scope of privacy is wider (than mere processing). However, it is broader because it applies to the processing of personal data, even if such processing doesn't impinge upon the privacy of an individual."

[70] JEU, Case C-139/01, Österreichischer Rundfunk and Others,

[71] Raphaël Gellert, Serge Gutwirth, The legal construction of privacy and data protection, Computer Law & Security Review, Volume 29, Issue 5, October 2013, Pages 522-530

FIGURE 5: PRIVACY AND DATA PROTECTION



Under EU law, the right to privacy and the right to data protection are recognised as at least formally distinct (although some overlaps may exist) under different legal instruments. Further, both these rights are accorded the status of fundamental rights. However, the position of these two rights under Indian law is different. The Supreme Court of India has expressly recognised the right to privacy as a fundamental right[72] but has not expressly accorded the same status to the right to data protection. However, the Court has held that privacy has both positive and negative content. The negative content restrains the state from committing an intrusion upon the life and personal liberty of a citizen. Its positive content imposes an obligation on the state to take all necessary measures to protect the individual's privacy[73]. Further, it has held that informational privacy is a facet of the right to privacy[74].

In Puttuswamy I, the Supreme Court recognised that the sphere of privacy stretches to the right to be left alone, while a broader connotation is related to the protection of one's identity. Data protection relates closely with the latter sphere. Apart from safeguarding privacy, data protection regimes seek to protect the autonomy of the individual[75]. Therefore, it stated that formulating a regime for data protection needs a "careful balancing of the requirements of privacy coupled with other values which protect data sub-serves together with the legitimate concerns of the State[76]." The state's legitimate aims would include protecting national security, preventing and investigating crime, encouraging innovation and the spread of knowledge, and preventing the dissipation of social welfare benefits[77]. Justice D.Y. Chandrachud in his judgement expressly stated:

[72] K.S. Puttuswamy v. Union of India, Writ Petition (Civil) No. 494 of 2012, Supreme Court of India, decided on August 24, 2017 (hereinafter referred to as Puttuswamy I)

[73] Puttuswamy I, Justice D.Y. Chandrachud for himself and Justice Jagdish Chandra Kehar, Justice R.K. Agrawal and Justice S. Abdul Nazeer, Part T, para 3(I)

[74] Puttuswamy I, Justice D.Y. Chandrachud for himself and Justice Jagdish Chandra Kehar, Justice R.K. Agrawal and Justice S. Abdul Nazeer, Part T, para 5

[75] Puttuswamy I, Justice D.Y. Chandrachud for himself and Justice Jagdish Chandra Kehar, Justice R.K. Agrawal and Justice S. Abdul Nazeer, para 177

[76] Puttuswamy I, Justice D.Y. Chandrachud for himself and Justice Jagdish Chandra Kehar, Justice R.K. Agrawal and Justice S. Abdul Nazeer,Part S, para 179

[77] Puttuswamy I, Justice D.Y. Chandrachud for himself and Justice Jagdish Chandra Kehar, Justice R.K. Agrawal and Justice S. Abdul Nazeer,Part T, para 5

"...the State may have justifiable reasons for the collection and storage of data. In a social welfare state, the government embarks upon programmes which provide benefits to impoverished and marginalised sections of society. There is a vital state interest in ensuring that scarce public resources are not dissipated by the diversion of resources to persons who do not qualify as recipients. Allocation of resources for human development is coupled with a legitimate concern that the utilisation of resources should not be siphoned away for extraneous purposes. Data mining with the object of ensuring that resources are properly deployed to legitimate beneficiaries is a valid ground for the state to insist on the collection of authentic data. But, the data which the state has collected has to be utilised for legitimate purposes of the state and ought not to be utilised unauthorizedly for extraneous purposes. This will ensure that the legitimate concerns of the state are duly safeguarded while, at the same time, protecting privacy concerns. Prevention and investigation of crime and protection of the revenue are among the legitimate aims of the state. Digital platforms are a vital tool of ensuring good governance in a social welfare state. Information technology – legitimately deployed is a powerful enabler in the spread of innovation and knowledge[78]."

Ultimately, the creation of a data protection regime remains the prerogative of Parliament. However, the Supreme Court has set the ball rolling by determining certain issues which the data protection framework must address. It has also brought to the fore concepts of anonymity[79] and the right to be forgotten[80], all of which will have to be elaborated further, either by court decisions in future or through legislation.

[78] Puttuswamy I, Justice D.Y. Chandrachud for himself and Justice Jagdish Chandra Kehar, Justice R.K. Agrawal and Justice S. Abdul Nazeer,Part S, para 181

[79] Puttuswamy I, Justice D.Y. Chandrachud for himself and Justice Jagdish Chandra Kehar, Justice R.K. Agrawal and Justice S. Abdul Nazeer,Part S, para 182

[80] Puttuswamy I, Justice Sanjay Kishan Kaul, para 69

CHAPTER 6

BALANCING TRANSPARENCY AND PRIVACY IN JUDICIAL PROCEEDINGS

A. BALANCING OF RIGHTS

The recognition of right to privacy as a fundamental right may, at times, limit the open court principle. It is possible that circumstances may emerge which will necessitate the balancing between these two equally important rights. However, as a general rule, it can be asserted that open courts cannot be regarded as being violative of the fundamental right to privacy because:

(i) the principle of open courts is widely recognised under various laws[81];

(ii) it seeks to achieve a legitimate state interest, i.e. fairness in the administration of justice[82]; and

(iii) it is proportional because the principle has a rational nexus with achieving fairness in the administration of justice through transparency and inspiring public confidence in the judicial process.

When public trial conflicts with other equally important rights which are essential in the interest of administration of justice, open courts may be regulated or controlled[83]. Courts in India have until now maintained the delicate balance between open courts and the right to privacy by conducting in-camera trials, prohibiting and restricting certain reporting, publication and dissemination of information, and regulating access to court records under its own rules and the Right to Information Act. These are discussed in further detail later in Chapter VI part B-D of this paper. Therefore, open courts do not disproportionately impact the rights held by the people.

[81] Section 153B of the Code of Civil Procedure and Section 327(1) of the Code of Criminal Procedure, Article 145(4) of the Constitution

[82] Naresh Sridhar Mirajkar v. State of Maharashtra, AIR 1967 SC 1

[83] Naresh Sridhar Mirajkar v. State of Maharashtra, AIR 1967 SC 1

In the digital environment however, the question is how a system of online access might be designed to ensure a balance between access to court records and the underlying rationale for the right to open courts while protecting privacy. In addition courts should embrace opportunities and minimise new risks that were not present in the paper-based world and are unique to the digital environment.

The Supreme Court in *Swapnil Tripathi v. Supreme Court of India*, in the context of live-streaming of court proceedings has categorically stated that it was mindful of the balance that has to be struck between various interests regarding administration of justice, including open justice, dignity and privacy of the participants to the proceedings and the majesty and decorum of the Courts. It stated that while live-streaming would be an affirmation of the constitutional rights bestowed upon the public and the litigants, regard must be had to the fact that it may not be desirable to live stream proceedings where privacy rights of the litigants or witnesses whose cases are set down for hearing may affect the cause of administration of justice itself. The regulatory framework should provide for a sincere effort to harmonise the competing claims in the event of a conflict between the two rights. Such harmonisation should give maximum expression to each right while minimising the encroachment on the other rights. The Court then stated that only court-directed matters can be heard in camera. In the absence of such a direction, the hearing of the will be in open court and by virtue of live streaming of court proceedings, such open court proceedings would go public beyond the four walls of the courtroom. However, if the party or a witness to the proceedings has genuine reservations, it can claim the right of privacy and dignity. Such a claim will have to be examined by the concerned Court, and for which reason, a just regulatory framework must be provided for, including obtaining the prior consent of the parties to the proceedings to be live streamed[84]. Justice D.Y. Chandrachud listed the following classes of cases to be excluded from live streaming – (a) matrimonial matters, including transfer petitions; (b) cases involving sensitive issues in the nature of sexual assault; and (c) matters where children and juveniles are involved, like POCSO cases[85]. Moreover, the Court was also vested with the power to disallow/ suspend the live-streaming for specific cases in whole or in part, suo motu or on an application filed by any party to the proceeding or otherwise, keeping in mind that the cause of administration of justice should not suffer in any manner[86].

84 Swapnil Tripathi v. Supreme Court of India, (2018) 10 SCC 628, para 13

85 Swapnil Tripathi v. Supreme Court of India, (2018) 10 SCC 628, Justice D.Y. Chandrachud, para 26(1)(a)

86 Swapnil Tripathi v. Supreme Court of India, (2018) 10 SCC 628, para 14(iii)

Transparency and privacy can be balanced through limitations on the access and use of personal information arising in the context of judicial proceedings. We must rethink what information in court records should be made public and regulate the uses of such records. If we abandon the notion that privacy is an exclusive status and recognise that personal information in court records can still remain private even if there is limited access to it, then a workable compromise for the tension between transparency and privacy emerges[87]. The solution is not to eliminate all access to court records or to exclude entire categories of documents from public access, but to redact/anonymise/mask personal information to the extent necessary. As a general rule, access should be granted for uses furthering traditional functions of transparency such as the watchdog function; access should be denied for commercial solicitation uses because such uses do not adequately serve the functions of transparency.

B. IN-CAMERA TRIALS

In-camera proceedings are generally held in sensitive cases essentially to protect the privacy of the parties. Simply put, an in-camera proceeding is a proceeding carried out in private, in the absence of the public and the press. It has been giving statutory backing in several instances, particularly cases involving sexual crimes and domestic life. In-camera trials are allowed in sexual assault cases[88], divorce proceedings[89], domestic violence cases[90], cases involving juveniles[91], and in the interest of the sovereignty, integrity and national security[92].

[87] Daniel J. Solove, Access and Aggregation: Privacy, Public Records, and the Constitution, 86 Minn. L. Rev. 1137 (2002)

[88] Section 327 of the Code of Criminal Procedure

[89] Section 22 of the Hindu Marriage Act, 1955; Section 33 of the Special Marriage Act, 1954, Section 11 of the Family Courts Act, 1984 and Section 43 of the Parsi Marriage and Divorce Act, 1936

[90] Section 16 of the Protection of Women from Domestic Violence Act, 2005

[91] Section 228 of the Indian Penal Code (IPC) and Section 23 of the Protection of Children from Sexual Offences Act, 2012, Section 3(xi), Juvenile Justice (Care and Protection of Children) Act, 2015

[92] Section 44 of the Unlawful Activities (Prevention) Act, 1967; Section 17 of the National Investigation Agency Act, 2008 and Section 14 of the Official Secrets Act, 1923

In-camera proceedings are an exception to the rule of open court. In *Naresh Shridhar Mirajkar v. State of Maharashtra*, the Supreme Court upheld the law allowing an in-camera trial. The law was held to not violate the fundamental right of speech because the person restrained is legally prevented from entering the Court and hearing the proceedings, and the liberty of speech is affected only indirectly.[93] Further, even if in-camera trials trespass on the right of movement, it would be protected under Article 19(5) which permits laws to be made imposing reasonable restrictions on that right in the 'interests of the general public'. The power to hold trials in-camera can be exercised only in the interests of administration of justice and there can be no doubt that administration of justice is a matter of public interest.

While certain statutes make in-camera proceedings mandatory[95], some statutes give discretion to the courts to determine the necessity of holding proceedings in-camera[96]. Discretion arises in two circumstances. Firstly, the discretion is vested on the courts by a law, for example, both the civil and criminal procedure code permit the judge/authority to depart from open courts if they think fit[97]. And secondly, the Courts have the inherent power to depart from the principle of open courts if fair administration of justice so requires[98].
It has been emphasised that the power to hold in-camera proceedings must be exercised with great caution and it is only if the court is satisfied beyond a doubt that the ends of justice themselves would be defeated if a case is tried in open court[99]. This requires exercise of due care and caution before the court directs the trial out of the public gaze[100]. Further, the Court cannot exercise its discretion to hear cases in camera, even when all parties consent, except in special cases in which a hearing in open court might defeat the ends of justice.

One notable example where the Supreme Court exercised its discretion to hold in-camera proceedings was in the context of the contents of the Radia tapes (transcripts of tapped conversations of lobbyist Nira Radia with businessman Ratan Tata and several bureaucrats, politicians and journalists). Ratan Tata had contended that the unauthorised publication of a private conversation between two citizens fell afoul of the right to privacy under the Indian Constitution. This case brought to the fore the interesting issue of an individual's right to privacy weighed against the public's right to know. Though there were clearly some private elements in the leaked conversations, the very reason these tapes caused a furore and were detrimental to Ratan Tata's reputation was the fact that they affect issues of public interest, i.e. the manner in which the democratic system was allegedly subverted by a small group of powerful people in the public sphere – journalists, businessmen and politicians. The overall character of these conversations seemed to be dealing with issues of public interest, which the public arguably has a right to know and the media an obligation to responsibly report and publish. This is an integral part of the fundamental right of freedom of expression, which needs to be balanced with the right to privacy.

[93] Naresh Shridhar Mirajkar v. State of Maharashtra, (1966) SCR (3) 744
[94] A. K. Gopalan v. The State, AIR 1950 SC 27
[95] Section 37 of the Protection of Children from Sexual Offences Act, 2012, Section 327(2) of the Code of Criminal Procedure
[96] Section 153B of the Code of Civil Procedure and Section 327(1) of the Code of Criminal Procedure
[97] Section 153B of the Code of Civil Procedure and Section 327(1) of the Code of Criminal Procedure
[98] Naresh Sridhar Mirajkar v. State of Maharashtra, AIR 1967 SC 1
[99] Naresh Shridhar Mirajkar v. State of Maharashtra, (1966) SCR (3) 744
[100] Janaki Ballav v. Bennet Coleman and Co. Ltd. AIR 1989 Orissa 225

The law empowering a Court to prohibit publication of its proceedings is a facet of the power to hold a trial in-camera and stems from it. It is protected by Article 19(2) of the Constitution which states that a law may validly impose reasonable restrictions on the liberty of speech, if it is in relation to contempt of court. When the court or a law in the interests of justice prohibits the publication of court proceedings and such prohibition is disobeyed, it amounts to an obstruction to the course of justice and contempt of the court[101].

The prohibition on publication of court proceedings usually arises from two sources:

1) Since courts have the inherent power to hold trials in-camera, and the power to prohibit publication is a facet of such power, the courts have the ability to prohibit the publication of proceedings in exercise of their inherent powers.

2) Sometimes, the statutes themselves prescribe a prohibition or limitation on the publication of court proceedings. However, even in such cases, the Court is generally empowered to varying degrees to permit such publication. For example, under Section 22 (1) of the Hindu Marriage Act, as a general rule all proceedings under the act must be conducted in-camera and it is unlawful for any person to print or publish any matter in relation to any such proceeding.

> “Since courts have the inherent power to hold trials in-camera, and the power to prohibit publication is a facet of such power, the courts have the ability to prohibit the publication of proceedings in exercise of their inherent powers. Sometimes, the statutes themselves prescribe a prohibition or limitation on the publication of court proceedings[103].”

[101] Naresh Shridhar Mirajkar v. State of Maharashtra, (1966) SCR (3) 744

[102] Section 7(1)(a) and (b), Contempt of Court Act

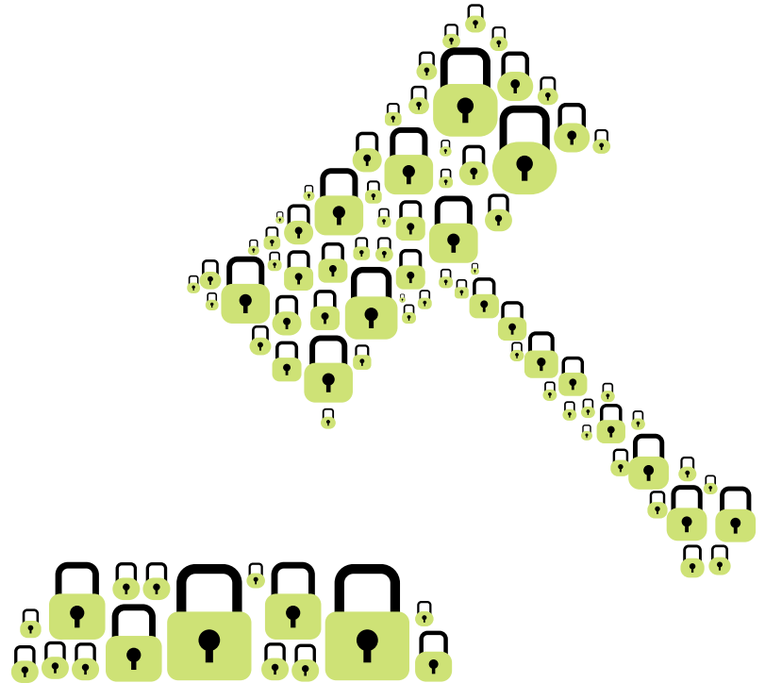
[103] Section 7(2) Contempt of Court Act

In *R. Rajagopal v. State of Tamil Nadu*[104], the Supreme Court held that a citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child-bearing and education among other matters. No one can publish anything concerning the above matters without his consent whether truthful or otherwise and whether laudatory or critical. If they do so, they would be violating the right to privacy of the person concerned and would be liable in an action for damages. The position may, however, be different, if a person voluntarily thrusts himself into controversy or voluntarily invites or raises a controversy. Further, if publication is based upon public records including court records, the right to privacy no longer subsists as the matter becomes a matter of public record and it becomes a legitimate subject for comment by press and media among others.

In Puttuswamy I, the court has referred to the above observations made in R. Rajagopal v. State of Tamil Nadu and has not expressed any disagreement with it. Therefore, it can be argued that the Court endorses the position of law that no right of privacy can be claimed in case of publication or reporting that is based on public records, including court records.

Further, it was held in *R. Rajagopal v. State of Tamil Nadu* that in the case of public officials, right to privacy is not available with respect to their acts and conduct relevant to the discharge of their official duties. In matters not relevant to the discharge of official duties, the public official enjoys the same protection as any other citizen. However, the judiciary, which is protected by the power to punish for contempt of court and the Parliament and legislatures protected as their privileges are by Articles 105 and 104 respectively of the Constitution of India, represent exceptions to this rule.

It has been observed that courts in some instance have not followed the aforementioned position with regard to public officials in its true spirit. For example, in the Saradha chit fund scam, the High Court of Calcutta agreed to hear the anticipatory bail prayer of former Calcutta Police Commissioner Rajeev Kumar in-camera despite the fact that he had been accused by the CBI of tampering with evidence and shielding influential persons involved in the illegal scheme. Rajeev Kumar was the head of the special task force in charge of the investigation of the scam and was therefore acting in his capacity as a public official[105].



[104] R. Rajagopal v. State of Tamil Nadu, 1994 SCC (6) 632

[105] Ravik Bhattacharya, 'Explained: Who is Rajeev Kumar, Saradha linked IPS officer who is now CBI's most wanted', The Indian Express, 20 September 2019, available at: https://indianexpress.com/article/explained/explained-who-is-rajeev-kumar-saradha-linked-ips-officer-who-is-now-cbis-most-wanted-6013226/

D. COURT RECORDS

(i) Are court records public documents?

Section 74 of the Evidence Act defines a public document as including documents forming the acts, or records of the acts of the sovereign authority, of official bodies and tribunals, and of public officers, legislative, judicial and executive. Therefore, in accordance with the above definition, court records should constitute public records. However, at this juncture it becomes important to distinguish between the record of the act of the Court and the record of the Court. In *State of Gujarat v. Ambalal Maganlal Shah*[106], the Court, as early as in the year 1965, explained this distinction in the following words:

"A private document does not become a public document simply because it is filed in the Court. To be a public document, it should be a record of the act of a public officer or Court. There is a distinction between the record of the act of the Court and the record of the Court. A document which forms part of the record of the Court does not necessarily form record of the act of the Court. It may be that upon a private document, which is a record of the act of private parties, a second act is done by the public officer or by the Court, namely filing the document or putting a number on the document. Only that portion of the document, which records the act of the Court in filing the document would be a public document. Therefore, that part of the document, namely the original part would be a private document forming the record of the act of the private parties and what is subsequently added to that document by the Court would be a public document."

> **Not all documents in the custody of courts constitute public records. Only those documents which either constitute the act of the court or record such acts acquire a public character. Therefore, a private document continues to retain its private character even if it forms part of the case file, unless the court or its officers perform some actions on such documents in the usual course of their official duties.**[103]

[106] State of Gujarat v. Ambalal Maganlal Shah, 1965 SCC Online Guj 197

In other words, not all documents in the custody of courts constitute public records. Only those documents which either constitute the act of the court or record such acts acquire public character. Therefore, a private document continues to retain its private character even if it forms part of the case file, until and unless some actions are performed by the court or its officers on such documents in the usual course of their official duties. Just because a document is filed before a Court in any form, it does not acquire a 'public' character. In fact, it is not the record of the Court, rather, the record of acts of the Court which is considered as a public document. Clearly, orders or decrees passed by the Courts are public documents, as they are the record of the acts of such Courts. As pleadings or other private documents (like affidavits and evidence) filed before the various Courts do not constitute an 'act of the court', would such documents then be considered 'public'?[107] What happens when the contents of the pleading are read out by the lawyers in open court? Does this impart a public character to such documents? Arguably, yes. While it is completely legal for anyone to sit in a courtroom and take notes while a lawyer narrates the contents of the pleadings before an open court, it is difficult to understand why pleadings are not accessible in a simple manner. In his dissenting opinion in Naresh Mirajkar case, Justice Hidayatullah expressed that if the matter is already published in open court, it cannot be prevented from being published outside the courtroom. It is only when the public is excluded from the audience that the privilege of publication also goes because the public outside then have no right to obtain second-hand what they cannot obtain in the court itself[108]. Extending this rationale, it can be argued that pleadings and transcripts should be generally made publicly accessible, subject to certain restrictions needed to preserve other competing interests such as fair and impartial administration of justice.

[107] Varun Sharma and Abhishek Goyal, 'Fate of Private Document Kept in Public File', Mondaq, 19 September 2018, available at: https://www.mondaq.com/india/trials-appeals-compensation/737408/fate-of-private-document-kept-in-public-file#:~:text=Therefore%2C%20that%20part%20of%20the,a%20document%20is%20filed%20before

[108] Naresh Shridhar Mirajkar v. State of Maharashtra, (1966) SCR (3) 744

(ii) Preserving privacy in court records

In *District Registrar and Collector, Hyderabad v. Canara Bank*, the Court repudiated the notion that a person who places documents with a bank would, as a result, forsake an expectation of confidentiality. In the Court's view, even if the documents cease to be at a place other than in the custody and control of the customer, privacy attaches to persons and not places, and hence the protection of privacy is not diluted. Parting with information to a third party (in this case, the bank) does not deprive the individual of the privacy interest. The reasonable expectation is allied to the purpose for which information is provided.

The reasoning of the court can be extended to support the position that mere filing of documents containing personal information before the courts does not extinguish the expectations of privacy of the person submitting such information. Admittedly, the Supreme Court itself has observed that information held by the High Court on the judicial side is the personal information of the litigants, which it holds as a custodian for the purpose of adjudication. The appropriate balance of privacy and transparency requires that third parties seeking information other than that published in orders and judgments must file an application/affidavit to obtain information/ certified copies of the documents as per the High Court's rules[109].

Courts in India have thus taken a case-by-case approach to balance the right of access to judicial records and privacy concerns arising out of personal information contained in such records.

Privacy of non-parties and third parties whose information is contained in judicial records

In *Naresh Sridhar Mirajkar v. State of Maharashtra*[110], a witness (non-party) in a defamation case against the editor of a weekly newspaper had requested the Court to order that no publicity be given to his evidence in the press as his business would be affected. After hearing arguments, the trial judge passed an oral order prohibiting the publication of the evidence. The order was challenged before the Supreme Court, which held that since the order was passed to help the administration of justice to obtain true evidence in the case, the order was within the court's inherent power.

In *Laksh Vir Singh Yadav v. Union of India*, a case pending before the High Court of Delhi, the petitioner has sought that he be "delinked" from information regarding a criminal case involving his wife and mother, which was eventually settled. Although the petitioner wasn't a party in the case, his name was nevertheless mentioned in the court order. As the details of the court proceedings were available online, the case showed up in the results whenever the petitioner's name was searched on the internet. The petitioner has complained that this could potentially affect his employment opportunities. The petitioner has also approached IndianKanoon, a legal database, to remove the order (related to the case being settled) from its website and Google for removing the link to the judgment from its search engine[111].

[109] Chief Information Commissioner v. High Court of Gujarat, (2020) 4 SCC 702

[110] Naresh Sridhar Mirajkar v. State of Maharashtra, AIR 1967 SC 1

[111] Laksh Vir Singh Yadav v. Union of India, Writ Petition (Civil) 1021 of 2016 , Delhi High Court

Personal/sensitive personal information contained in judicial records

In *P. Gopalkrishnan @ Dileep v. State of Kerala*[112], the Court held that the contents of a memory card/pen drive containing footage of an alleged occurrence of rape, being an electronic record must be regarded as a document and if the prosecution is relying on the same, ordinarily, the accused must be given a cloned copy thereof to enable him/her to present an effective defence during the trial. However, in cases involving issues such as the privacy of the complainant/ witness or his/her identity, the Court may be justified in providing only inspection thereof to the accused and his/her lawyer or expert for presenting effective defence during the trial. The Court may issue suitable directions to balance the interests of both sides.

In *CPIO, Supreme Court of India v. Subhash Chandra Agarwal*[113], the Supreme Court held that furnishing information on the judges of the Supreme Court who had declared their assets would not, in any way, impinge upon the personal information and right to privacy of the judges. The Court held that the public interest test in the context of the RTI Act would mean reflecting upon the object and purpose behind the right to information, the right to privacy and consequences of invasion, and breach of confidentiality and possible harm and injury that would be caused to the third party, regarding particular information and the person. After a perusal of judicial precedents under the RTI Act, the Court observed that personal records, including name, address, physical, mental and psychological status; educational records; professional records; medical records, including those of the family members[114]; and detailed private financial records are all personal information. Such information is entitled to protection from unwarranted invasion of privacy, and conditional access is available when stipulation of larger public interest is satisfied.

[112] P. Gopalkrishnan @ Dileep v. State of Kerala and Another, Criminal Appeal No. 1794 of 2019, High Court of Kerala

[113] CPIO, Supreme Court of India v. Subhash Chandra Agarwal, Civil appeal no. 10044 and 2683 of 2010, Supreme Court of India, November 13, 2019

[114] The Delhi High Court has passed a judgment on medical records in this context. LPA 34/2015 and C.M. No. 1287/ 2015, High Court of Delhi, April 17, 2015

Right to be forgotten, De-identification, and Anonymization

In *CPIO, Supreme Court of India v. Subhash Chandra Agarwal*[115], it was held that "privacy and confidentiality encompass a bundle of rights including the right to protect identity and anonymity." Anonymity is where an individual seeks freedom from identification, even when and despite being in a public space. The courts have directed the press, media, and law journals to anonymize names of parties (for example, reporting the names as 'X' and 'Y') in several instances such as a bail matter about a sexual harassment complaint[116], names of husband and wife in a divorce case[117], names of the parties in a case for payment of maintenance where parentage had to be ascertained through a DNA test[118], and the name of an HIV positive patient and the name of the hospital where such patient was treated[119].

In a case before the High Court of Gujarat, the Court ordered the modification of an order to remove the names of the minor children and delete/amend their medical information. The Court also stated that requests of the applicant before the law journals and media not to publish the original order 'may' be considered by the webmasters in the particular interest and well-being of the children. The order of the Court seems only directory in nature and not binding[120].

In *Sri Vasunathan v. The Registrar General*[121], the Karnataka High ordered the removal of the petitioner's daughter's name from an earlier order passed by the Court, as she feared this court order would appear in search engine results, potentially harming her marital relationship, reputation, and goodwill. The Court observed that this would be in line with the trend in western countries where the 'right to be forgotten' was followed as a matter of rule in sensitive cases. The Court directed the Registry to mask her name in the cause title and anywhere in the body of the order passed by the Court before releasing the order for the benefit of any other service provider who may seek a copy of the order. However, the Court ordered that no such masking of the name would be carried out while publishing the order on the High Court website, and consequently, the name of the petitioner's daughter would be reflected in certified copies of the court order.

The Kerala High Court has recently admitted a petition seeking the erasure of a person's personal details from a bail order available on the internet, from a case in which they were acquitted[122].

In *Jorawer Singh Mundy v. Union of India*[123], the Delhi Court granted interim protection to an American citizen of Indian origin by directing IndianKanoon to block the judgement of his acquittal under NDPS Act from being accessed by using search engines such as Google/Yahoo etc. The case of the petitioner was that despite him having a good academic record, he was unable to get any employment opportunity up to his expectations due to the availability of the said judgement online.

[115] CPIO, Supreme Court of India v. Subhash Chandra Agarwal, Civil appeal no. 10044 and 2683 of 2010, Supreme Court of India, November 13, 2019

[116] 'X' v. 'Y', Criminal Original Petition No. 932 of 2014, Madras High Court

[117] 'X' v. 'Y', Family Court Appeal No. 133 of 2006, Bombay High Court, March 7, 2014; Master 'X' v. 'Y', AIR 2003 Delhi 195, March 17, 2003

[118] Master 'X' v. 'Y', AIR 2003 Delhi 195, March 17, 2003

[119] Mr 'X' v. Hospital 'Z', Appeal (Civil) 4641 of 1998, Supreme Court of India, September 21, 1998

[120] Criminal Misc. Application (Modification of Order) No. 1 of 2019 in R/ Special Criminal Application No. 1627 of 2016 dated 21 June 2019

[121] Sri Vasunathan v. The Registrar General, Writ Petition 62038 of 2016 (GM-RES), Karnataka High Court, January 23, 2017

[122] Lydia Suzanne Thomas. 2020. 'Right to be forgotten: Kerala High Court admits petition for removal of personal information from court order available on Google', Bar & Bench, 19 October, available online at https://www.barandbench.com/news/litigation/kerala-high-court-admits-plea-removal-personal-information-google (accessed on 28 December 2020).

[123] Jorawer Singh Mundy v. Union of India, Writ Petition (Civil) 3918/ 2021, April 12, 2021, Delhi High Court

(iii) Current framework to access court records

The current framework to access court records in India can be broadly categorized into the following streams of access:

1. Applications under the rules made by the courts, including the court's RTI rules
2. Applications under the Right to Information Act, 2005 (RTI Act) and proactive disclosure made by courts under the Act.

1. ACCESSING COURT RECORDS UNDER RULES FRAMED BY THE COURT

Courts in India typically provide a mechanism for copying and inspecting court records under their rules. These rules are slightly different for parties to a proceeding and non-parties.

a. Supreme Court of India

Order XIII of the Supreme Court Rules, 2013 lays down the procedure for granting certified copies of court records. A party to a proceeding is entitled to apply for and receive certified copies of all pleadings, judgments, decrees or orders, documents and depositions of the witnesses made or exhibited in the concerned proceeding by making appropriate application and paying the requisite fees.[124]. However, a person who is not a party to the case, appeal or matter whether pending or disposed, must make an application and show good cause on the basis of which the court may allow such person to receive copies of the aforementioned court records[125]. Further, no party or other person shall be entitled as of right to receive copies of or any extracts from any minutes, letter or document of any confidential nature or any paper sent, filed or produced, which the Court directs to keep in sealed cover or considers to be of confidential nature or the publication of which is considered to be not in the interests of public, except under and in accordance with a court order[126].

b. High Courts and district courts

High Courts provide a procedure for non-parties to a case to apply for copies or inspect the judicial records of that case, in the rules that they frame for themselves and the district courts within their jurisdiction.

Procedures and grounds of gaining access to judicial records

Parties to the proceedings are entitled to obtain certified copies of all documents after applying along with the prescribed court fees. They may be permitted to inspect and copy any document that is a part of the record. The application procedure, the level of restrictions they impose on access, and the level of authorisation required for a non-party to gain access varies between High Courts. Some require the filing of an affidavit that declares the applicant's interest in the subject matter of the document[127]. Rules may require the applicant to obtain a court order to authorise their access, which is issued based on the application (and the associated affidavit, if any)[128]. Some simply require that permission for inspection and copies must be given subject to the Registrar's satisfaction that the applicant has sufficient reason and justification to do so[129].

[124] Supreme Court of India Rules, 2013, Order XIII Rule 1
[125] Supreme Court of India Rules, 2013, Order XIII Rule 2
[126] Supreme Court of India Rules, 2013, Order XIII Rule 7
[127] Rule 118, Chapter X, Andhra Pradesh Civil Rules of Practice, 1990 (for inspection of documents only – also in use in Telangana High Court); Rule 108, Chapter VIII, Gujarat High Court Rules, 1993; Rule 200 (2), Chapter XIV, High Court of Chhattisgarh Rules, 2007; Rule 210, Chapter XXVIII, Madras High Court Criminal Rules of Practice, 2019
[128] Rule 5 (ii), Part III, Himachal Pradesh Civil and Criminal Courts (Preparation and Supply of Copies of Records) Rules, 2000; Rule 210, Chapter XXVIII, Madras High Court Criminal Rules of Practice, 2019; and in civil cases as per Rule 7, Order 6, General Rules (Civil & Criminal) 2017, Rajasthan High Court. The latter requires that the order is issued by the Presiding Officer of the court in question.
[129] Rule 200 (2), Chapter XIV, High Court of Chhattisgarh Rules, 2007; Rule 5 (ii), Part III, Himachal Pradesh Civil and Criminal Courts (Preparation and Supply of Copies of Records) Rules, 2000; Rule 212, Chapter XX, and Rule 227 (i), Chapter XXI, Jammu and Kashmir High Court Rules, 1999; Rules 344-346, Civil Court Rules of the High Court of Jharkhand; Rule 148, Part IV, Chapter I, Criminal Court Rules of the High Court of Jharkhand; Rule 1 (2), Chapter XVIII, the High Court of Madhya Pradesh Rules, 2008; Rule 2 (1), Chapter XII, Rules of the High Court of Meghalaya, 2013; Rules 208-210, Chapter VII, Sikkim High Court (Practice and Procedure) Rules, 2011; Rule 3, Chapter XIII and Rule 3, Chapter VIII, the Bombay High Court Appellate Side Rules, 1960, and Rule 268, Chapter XIX, Bombay High Court (Original Side) Rules, 1980

Notably, the rules of the High Courts of Andhra Pradesh, Telangana, Meghalaya, Patna, and Jharkhand require the applicant to show that access to court records is required for use in another court proceedings in which the applicant is a party[130]. The rules of Andhra Pradesh and Telangana High Courts specify that the application must provide information about the intended or pending case and describe the relevance of the documents to it[131]. If the application is submitted during the pendency of a case, the rules may require the applicant to establish sufficient urgency or even obtain an order of the court, to receive permission to inspect or make copies of the record[132].

Document-specific access

Many of the rules framed by the High Courts have different levels of restriction on access to the various documents that together constitute the judicial record. Applicants need not show sufficient reason to obtain copies of judgments and orders in some courts[133], but must do so in others, even though judgments and orders are publicly accessible on the courts' websites for High Courts, and the e-Courts Portal, for district courts[134].

Plaints, written statements, replies, affidavits, petitions, and memoranda of appeal are accessible upon application, as per the rules of most High Courts. While rules of some courts specifically state that applicants must show sufficient cause to access these documents[135], others state that these documents are available as of right upon payment of the prescribed fee[136]. In several High Courts, exhibits entered into evidence cannot usually be accessed without the consent of the party who filed such exhibits, or on the order of a judge when sufficient cause has been shown by the applicant[137]. Some courts require that good cause must be shown to obtain exhibits[138].

[130] Rule 118, Chapter X, Andhra Pradesh Civil Rules of Practice, 1990 (for inspection of documents only – also in use in Telangana High Court); Rule 2, Chapter XII, Rules of the High Court of Meghalaya, 2013; Rules 356-358 of Civil Court Rules of the High Court of Judicature at Patna; Rule 169, Criminal Court Rules of the High Court of Judicature at Patna; Rules 344-346, Civil Court Rules of the High Court of Jharkhand; Rule 148, Part IV, Chapter I, Criminal Court Rules of the High Court of Jharkhand;

[131] Rule 118, Chapter X, Andhra Pradesh Civil Rules of Practice, 1990 (for inspection of documents only – also in use in Telangana High Court)

[132] Rules 199 and 200 (b), Sikkim High Court (Practice and Procedure) Rules 2011; Rule 2, Order 6, General Rules (Civil & Criminal) 2017, Rajasthan High Court, and Rule 862, Chapter XXXVIII, Rules of the high Court of judicature at Rajasthan, 1952; Rule 216, Chapter XX, Jammu and Kashmir High Court Rules, 1999; Rule 341, Civil Court Rules of the High Court of Jharkhand; Rule 7, Himachal Pradesh Civil and Criminal Courts (Preparation and Supply of Copies of Records)Rules, 2000; Rule 40, Chapter XII, High Court of Manipur Rules, 2019

[133] Rules 7-8, Chapter XXXIX Allahabad High Court Rules, 1952, and Rule 253, Chapter X, General Rules (Civil), 1957, Allahabad High Court; Rule 10, Original Side Rules of the High Court of Calcutta, 1914, Rule 2(ii-iii), Part B, Chapter 5, Vol. 5, Delhi High Court Rules and Orders; Rule 2, Chapter XIII, Rules of the Gauhati High Court, 1954; Rule 5 (ii), Part III, Himachal Pradesh Civil and Criminal Courts (Preparation and Supply of Copies of Records)Rules, 2000; Rules 344-346, Civil Court Rules of the High Court of Jharkhand; Rule 2, Chapter XII, High Court of Manipur Rules, 2019, Rule 2, Chapter XII, Rules of the High Court of Meghalaya, 2013; "Rule 14, Chapter XXI, Orissa High Court Rules and Rule 352, Volume I, Orissa High Court General Rules and Circular Orders (Civil); Rules 357 of Civil Court Rules of the High Court of Judicature at Patna; Rule 3(2-2A) Punjab Civil and Criminal Courts Preparation and Supply of Copies of Records Rules, 1965; Rule 6 (for criminal cases) and Rule 7 (for civil cases), Order 6, General Rules (Civil & Criminal) 2017, Rajasthan High Court, and Rule 209 of the Sikkim Civil Courts Act, 1978.

[134] Rule 118, Chapter X, Andhra Pradesh Civil Rules of Practice, 1990 (also in use in Telangana High Court); Rule 200 (2), Chapter XIV, High Court of Chhattisgarh Rules, 2007; Rules 108 and 151, Chapter VIII, Gujarat High Court Rules, 1993; Rule 210, Chapter XXVIII, Madras High Court Criminal Rules of Practice, 2019; Rule 1 (2), Chapter XVIII, the High Court of Madhya Pradesh Rules, 2008

[135] Rule 212, Chapter XX, and Rule 227 (i), Chapter XXI, Jammu and Kashmir High Court Rules, 1999; Rules 245, Civil Court Rules of the High Court of Jharkhand

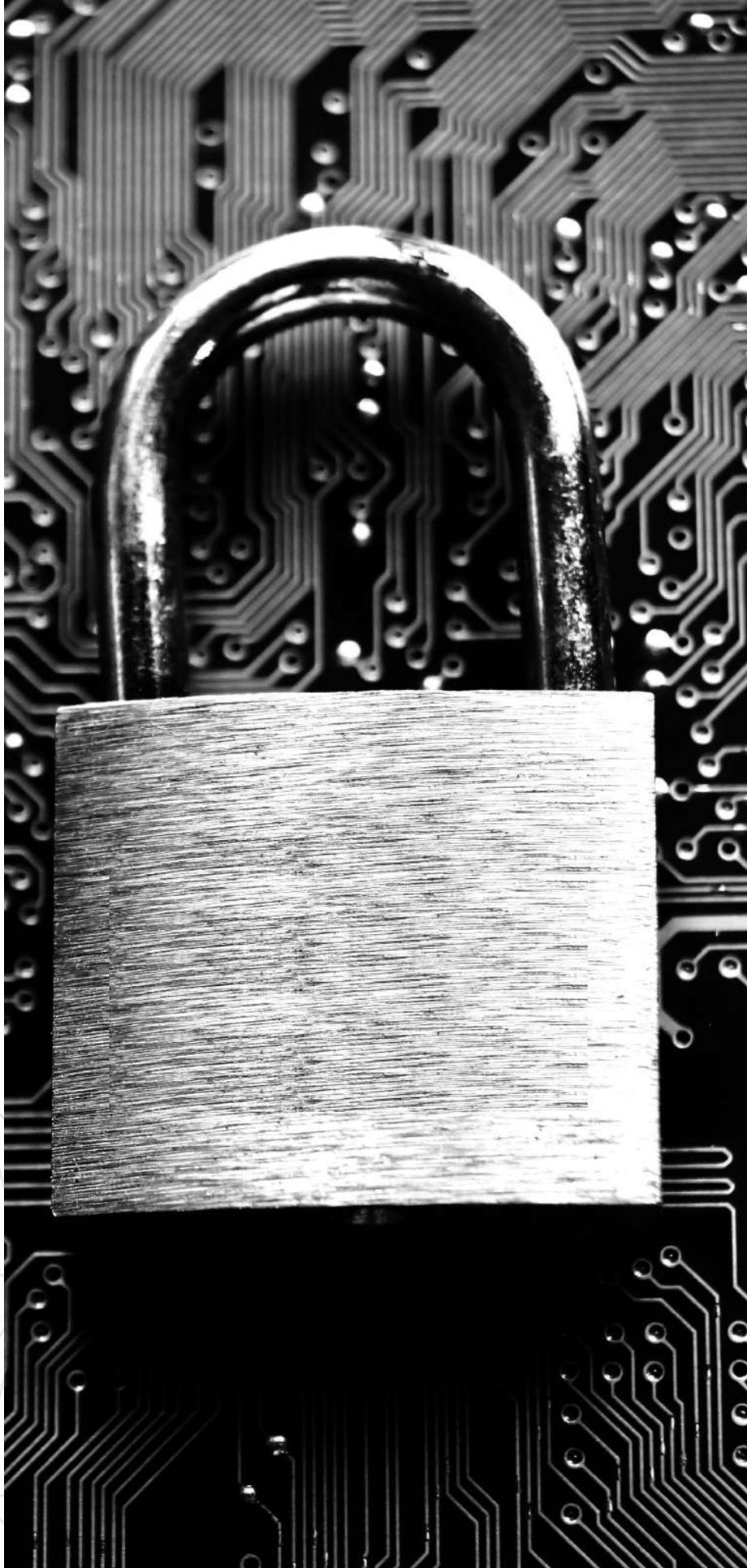
[136] Rule 2(ii), Part B, Chapter 5, Vol. 5, Delhi High Court Rules and Orders; Rule 3(2) Punjab Civil and Criminal Courts Preparation and Supply of Copies of Records Rules, 1965; Rule 208 of the Sikkim Civil Courts Act, 1978

[137] Rule 2(iv), Ch. 5, Part B, , Punjab and Haryana High Court Rules and Orders; Ch. XL, Rule 8 Allahabad High Court Rules, 1952; , and Rule 878, Rajasthan High Court Rules, 1952; Rule 2(iv), Part B, Chapter 5, Vol. 5, Delhi High Court Rules and Orders; Rule 10, Chapter 5, Gauhati High Court Criminal Rules and Orders; Rule 227(ii), Chapter XX, Jammu and Kashmir High Court Rules, 1999; Rule 4, Chapter XII, High Court of Manipur Rules, 2019; Rule 2(3), Chapter XII, Rules of the High Court of Meghalaya, 2013; Rule 353, Volume I, Orissa High Court General Rules and Circular Orders (Civil); Rules 210 of the Sikkim Civil Courts Act, 1978. As per Rule 5 (ii), Part III, Himachal Pradesh Civil and Criminal Courts (Preparation and Supply of Copies of Records) Rules, 2000, the requirement is not more strict for evidence than it is for other documents.

[138] Gauhati High Court, for criminal cases in district courts – see Rule 10, Chapter 5, Gauhati High Court Criminal Rules and Orders;

Principles and their implications

The intent behind these procedures is to ensure that non-parties can access documents in which they have a legitimate private interest. These rules allow for considerable discretion on the part of the court or its officer (e.g. Registrar) while determining whether an applicant has sufficient cause to need access to certain court records. While the Registrar or the Court may use their discretion to refuse access on grounds of privacy and sensitivity of information, very few courts' rules explicitly mention privacy as a ground for restricting access to information. Only some court rules, such as the Punjab and Haryana High Court, have specified instances in which records are not to be granted, such as in cases on the POCSO Act, sexual offences against women, rape cases and contempt matters[138].



[139] Rule 3(2A) Punjab Civil and Criminal Courts Preparation and Supply of Copies of Records Rules, 1965,

2. ACCESSING COURT RECORDS UNDER RIGHT TO INFORMATION ("RTI") ACT

a. Conflict between RTI and Court Rules

What happens in the case of a conflict between the procedure laid down by the RTI Act and the procedure laid down by the courts to access information? Section 22 of the RTI Act clearly states that the Act shall have an overriding effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force. However, there were conflicting decisions from the CIC and various High Courts as to which holds primacy - the RTI Act or the court rules. The Supreme Court ruling in *Chief Information Commissioner v. High Court of Gujarat and Another*[140] held that court documents on the judicial side cannot be accessed under RTI when the court rules provide for a specific mechanism[141]. The questions that arose for the courts' determination were:

A special enactment or rule cannot be held to be overridden by a later general enactment simply because the latter opens up with a non-obstante clause, unless there is clear inconsistency between the two legislations. In the absence of inherent inconsistency between the provisions of the RTI Act and the Gujarat High Court Rules, overriding effect of RTI Act would not apply. The Court opined that if any information can be accessed through the mechanism provided under another statute, then the provisions of the RTI Act cannot be resorted to as there is absence of the very basis for invoking the provisions of RTI Act, namely, lack of transparency. In other words, the provisions of RTI Act are not to be resorted to if the same are not actuated to achieve transparency.

This ruling sets a dangerous precedent and goes against the spirit of judicial transparency. It is necessary to understand the importance of court records to public discourse in India before critiquing the judgement and discussing its fall-out. Court decisions influence our daily life in myriad ways. Every prosecution before a criminal court is essentially an opportunity to hold the police accountable just as every writ petition is an opportunity to hold the government accountable. Similarly, a significant number of commercial lawsuits are opportunities to learn about corporations and how commercial transactions are executed in the country. In all of these cases, the pleadings filed by either party contain reams of information that are useful to a range of stakeholders such as citizens, journalists, academics, shareholders etc., who can better inform the public discourse on the ramifications of these decisions. This is also true of public interest litigations, where the courts may rely on the report of an amicus curiae or an expert committee. These reports unfortunately are not accessible by third parties, though they may be impacted by these decisions because they form part of the judicial record and hence outside the purview of the RTI Act.

[140] Chief Information Commissioner v. High Court of Gujarat and Anr., Civil appeal No(s). 1966-67 of 2020

[141] Chief Information Commissioner v. High Court of Gujarat and Anr., Civil appeal No(s). 1966-67 of 2020

The above decision reflects that the judiciary wishes to retain control over public accessibility of court records. However, the manner in which the Court has done so can lead to several problems:

1. Unlike RTI Act where locus standi does not matter and where no reasons have to be furnished to request information (which reduces the possibility of discretion), most court rules permit third parties to access court records only if they can justify their request to the satisfaction of the court.

2. While requests under RTI can be filed by post, the procedure under various court rules require physical filing of an application with the Registry, filing of supporting affidavits and sometimes a hearing before the judge to determine whether access should be granted. This presents a logistical barrier for those with limited means trying to gain access to court records[142].

3. By stating that the RTI Act cannot be used when the same information can be accessed through the mechanism provided under another statute, the Court is encouraging and enabling public authorities to bypass the RTI Act by providing for an alternative mechanism governing access in their governing statutes

.

> **“Therefore, if the power to control access to judicial records must remain with the judiciary, it should do so in clear terms (perhaps by an amendment in the RTI Act exempting disclosure of judicial records of the courts) and not through such ambiguous standard of legal reasoning which undermines the RTI Act and renders its non-obstante clause completely meaningless.”**

[142] Vidhi Centre for Legal Policy, ‘Open Courts in the Digital Age : A Prescription for an Open Data Policy.’

b. Types of court records accessible under RTI Act

Proactive disclosures

Under Section 4(1)(b) of the RTI Act, courts are required to proactively disclose certain information including information about their functions and duties, decision-making processes, documents held, employees' powers, and budgets held by it or under its control or used by its employees for discharging its functions, categories of documents that are held by it or under its control, the budget allocated to each of its agencies, indicating the particulars of all plans, proposed expenditures and reports on disbursements made, directory of its officers and employees, names, designations and other particulars of the Public Information Officers, etc. However, courts across India have shown varying degrees of compliance with this provision and often, the quality of the disclosure is deficient[143].

Other court records that may be sought

While the courts generally do respond to RTI requests for information regarding their administrative affairs, they do not provide copies of pleadings filed before them or other judicial records. *The Supreme Court in Chief Information Commissioner v. High Court of Gujarat and Another*[144] has clarified that information on the judicial side must be obtained through the mechanism provided under the High Court Rules, and the provisions of the RTI Act cannot be resorted to in such cases. Several High Courts have gone as far as drafting the Court Rules and the Court's RTI Rules under Section 28 of the RTI Act to expressly exclude disclosure of judicial records on an application made under the RTI Act[145]. For example, the Chhattisgarh High Court's RTI Rules state that information/ copy/ inspection concerning pending cases can be obtained only under the High Court rules and orders[146]. The Delhi High Court RTI Rules exempt from disclosure under the RTI route such information that relates to judicial functions and duties of the court[147]. The Civil Court Rules of Jharkhand High Court states that information relating to judicial records shall not be given on application filed under the RTI Act / Rules[148]. The Meghalaya High Court Rules, however stated that the judicial record is accessible through both the RTI Act and the procedure set under the rules themselves[149]. It is worth noting that Section 8(1)(j) of the Act contains an exemption from the disclosure of information which would cause an unwarranted invasion of the privacy of the individual.

[143] Vidhi Centre for Legal Policy. 2019. Sunshine in the Courts- Ranking the High Courts on Their Compliance With the RTI Act . Available online at https://vidhilegalpolicy.in/research/sunshine-in-the-courts-ranking-the-high-courts-on-their-compliance-with-the-rti-act/ (Accessed on 28 December 2020)

[144] Chief Information Commissioner v. High Court of Gujarat, Civil appeal No(s). 1966-67 of 2020

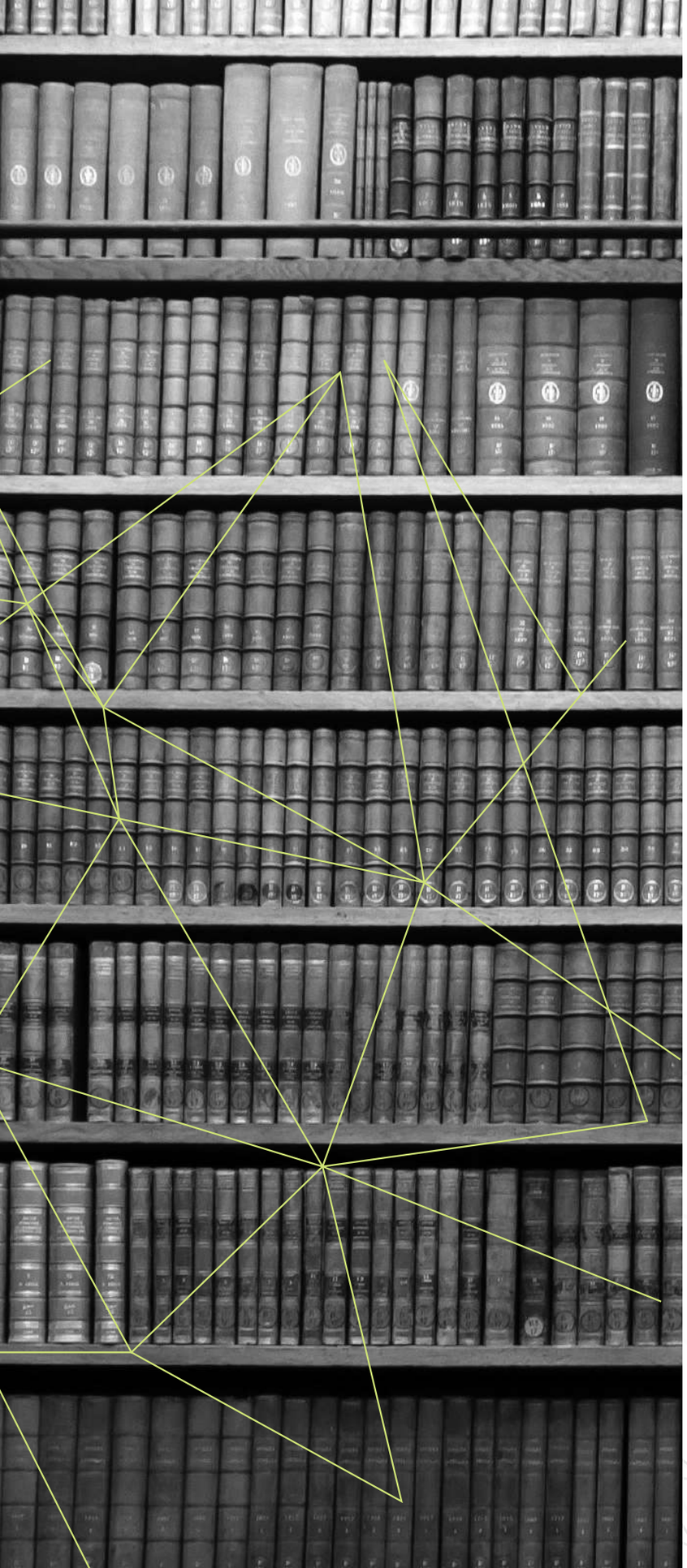
[145] Rule 5(a), Delhi High Court RTI Rules, 2006, Maharashtra District Court RTI rules, Delhi HC, Punjab and Haryana, Ch IV, R. 5(i), Odisha High Court RTI Rules, 2005

[146] Ch IV, R. 2, Chattisgarh High Court RTI Rules, 2005

[147] Rule 5(a), Delhi High Court RTI Rules, 2006

[148] Rule 338, Civil Court Rules of the High Court of Jharkhand

[149] Rule 5, Chapter IX, Rules of High Court Meghalaya, 2013.



Pleadings, orders and details of hearings

In *State Public Information Officer and Deputy Registrar (Establishment), High Court of Karnataka v. N. Anbarasm*[150], the petitioner had sought, inter alia, the following information related to certain writ petitions - number of hearings and number of times the writ petition was posted for hearing; procedure, guidelines and rules followed in posting the writ petitions; all orders passed by the judge; objections and written statements filed by the respondents; and early hearing application, memo and any other request made by petitioner's advocate. The High Court quashed the order of the State Information Commissioner passed pursuant to a complaint under Section 18 of the RTI Act which had directed the court to furnish the above information free of cost. The High Court held that since the petitioner was a party to the writ petitions in relation to which the above information was sought, he could obtain such information according to the rules of the High Court by making the necessary application and that the State Information Commissioner should have adverted to the High Court Rules.

Internal deliberations and minutes

In *Registrar General v. K. Elango*[151], the Madras High Court held that, "notings, jottings, administrative letters, intricate internal discussions, deliberations etc. of the High Court cannot be brought under Section 2(j) of the RTI Act. It also observed that if such information is made available, it will impede and hinder the regular, smooth and proper functioning of the institution namely, the High Court.

In *Registrar General v. R.M. Subramanian*[152], through a bunch of information requests, an applicant sought copies of files and minutes of meetings of judges of the Madras High Court relating to a criminal contempt petition that had been filed against a tahsildar and other public servants in relation to a property dispute. The Tamil Nadu State Information Commission directed the applicant to seek information in accordance with the Court's own rules instead of the RTI Act. A Division Bench of the Madras High Court ruled against disclosure of the information under RTI Act for the purpose of "maintaining utmost confidentiality and secrecy of the delicate function of the internal matters of High Court...if copies of the minutes dated ...are furnished, then, it will definitely make an inroad to the proper, serene function of the High Court being an independent authority under the Constitution of India."

[150] High Court of Karnataka v. N. Anbarasm, Writ petition No 9418/2008(GM-Res)

[151] Registrar General v. K. Elango W.P.No.20485 of 2012 and M.P.No.1 of 2012, Madras High Court, April 17, 2013

[152] Registrar General vs R.M. Subramanian, W.P.No.28643 of 2012 and M.P.No.1 of 2012, Madras High Court, June 14, 2013

Personnel Records

In *R.K. Jain v. Union of India*[153], the applicant wanted to access documents relating to annual confidential reports (ACRs) of a member of Customs Excise and Service Tax Appellate Tribunal and follow up action taken by the authorities based on the ACRs. The information sought was treated as personal information, which, except in cases involving overriding public interest, could not be disclosed. It was observed that the procedure under Section 11 of the RTI Act in such cases has to be followed. The matter was remitted to the Information Commissioner to examine the aspect of larger public interest and to follow the procedure prescribed under Section 11 of the RTI Act which, it was held, was mandatory.

In *Anju Negi v. Supreme Court of India*[154], the appellant sought the copy of an attestation form furnished by a court officer in the Supreme Court of India at the time of joining its services. The CIC held that all the information any employee furnishes to the employer in fulfilment of mandatory obligations or by way of minimum eligibility conditions must be disclosed as such information, even if it contains personal details, cannot be classified as personal information. However,if an employee voluntarily furnishes more personal details than mandated by the recruitment rules of the public authority concerned, the CPIO will not be obliged to disclose such information, and such information would clearly fall in the category of personal information having no relationship to any public activity or interest.

The following table summarizes the different avenues for gaining access to court records explained above

[153] R.K. Jain v. Union of India and Another, SLP(C)No.22609 of 2012, Supreme Court of India, April 16, 2013

[154] Anju Negi v. Supreme Court of India, File No.CIC/SM/A/2011/002810 & CIC/SM/C/2011/001444, April 11, 2012

ACCESS MECHANISM	OVERVIEW
Inherent powers	Courts can invoke their inherent powers to depart from 'open courts' in the interests of 'administration of justice. 'Administration of justice' is determined by the courts on a case-by case basis depending on the facts of each case.
Statutes	Some statutes mandate the pronouncement of judgments in open court. Some also require proceedings to be held in-camera and/or prohibit publication of court proceedings as a general rule. However, even in such cases, the court may depart from the general rule favouring open courts. Most statutes give discretion to the courts to determine the necessity of departing from open courts.
Court Rules	Court rules often require non-parties to show a good/ sufficient cause (or a similar standard) in order to gain access to certain kinds of court records which are generally available to the parties to a case. The rules allow for considerable discretion on the part of the court or its officer (e.g. Registrar) while determining whether an applicant has a legitimate interest.
Right to Information	The RTI Act exempts the disclosure of information which has been expressly forbidden to be published by any court of law or tribunal or the disclosure of which may constitute contempt of court. This means that if the courts have exercised their inherent or statutorily granted powers to restrict the reporting of certain court proceedings, one cannot access such information through the RTI route. Hence, ultimately the court controls whether such information is publicly accessible or not. The RTI Act also exempts the disclosure of information which relates to personal information, the disclosure of which has no relationship to any public activity or interest, or which would cause unwarranted invasion of privacy of the individual unless the CPIO/SPIO/appellate authority is satisfied that the 'larger public interest' justifies the disclosure of such information. What constitutes 'larger public interest' is decided by the relevant authorities. Such discretion has been exercised by RTI authorities generally to grant access to administrative records of courts and refuse access to judicial records. The Supreme Court has also clarified that information on the judicial side must be obtained through the mechanism provided under the High Court Rules, if any, and not under the RTI Act. This again reflects that the courts have retained control over granting access to judicial records.

> **"The case-by-case approach to defining privacy does not provide certainty or the kind of safeguards that are available under a robust data protection regime, which respects individual autonomy. Further, the absence of a clear and consistent access policy is a significant impediment in gaining access to the information contained in court records."**

CONCLUSION

The concern that privacy will be used to weaken transparency and to conceal crimes and corruption is often voiced as an obstacle to instituting a firm privacy law. When privacy must be balanced against the cutting- edge imperatives of national security, efficiency, and entrepreneurship, privacy often comes up the loser. The list of privacy counterweights is long and growing. The recent additions of social media, mobile platforms, cloud computing, data mining, and predictive analytics now threaten to tip the scales entirely, placing privacy in opposition to the progress of knowledge[155]. In Puttuswamy I, the Supreme Court observed that the above narrative has relevance in the Indian context as the country is poised to move to a knowledge-based economy. The Court states, "...Information is the basis of knowledge. The scales must, according to this critique, tip in favour of the paramount national need for knowledge, innovation and development. These concerns cannot be discarded and must be factored in. They are based on the need to provide economic growth and social welfare to large swathes of an impoverished society." Further, the Court devotes considerable thought to the notion of informational privacy. It notes that formulation of a regime for data protection is a complex exercise which needs to be undertaken by the State after a careful balancing of the requirements of privacy coupled with other values which the protection of data sub-serves together with the legitimate concerns of the State. The court recognizes several privacy principles like notice, choice and consent, collection limitation, purpose limitation, access and correction, security, accountability etc which must inform the formulation of a data protection framework. Therefore, while Puttuswamy I confers privacy with the status of a fundamental right, it is equally cognizant of the legitimate state interests which may operate as a limitation on the right to privacy.

The fundamental right to know and the fundamental right to privacy overlap extensively. The existing mechanism (legislations and judgments) available in do not give either right primacy over the other. The principle of indivisibility of fundamental rights requires that both rights carry equal weight. While balancing fundamental rights may sound uncomplicated in theory, it is quite challenging in practice. However, the conflicts between these two rights can be mitigated

[155] Puttuswamy I, para 138; Julie E Cohen, "What Privacy Is For", Harvard Law Review (2013), Vol. 126, at page 1904

or at least minimized through the enactment of clear definitions in legislation, guidelines, techniques, and oversight systems[156]. The following steps can aid the balancing of the two fundamental rights:

1. Laws on privacy, access to information and data protection must have compatible definitions of personal information and appropriate public interest tests should be adopted that allow for careful balancing of the two rights. In the Indian context, this would mean harmonizing the concepts under the Right to Information Act, 2005 and the proposed data protection frameworks in the form of the Personal Data Protection Bill, 2020 and the Report on Non-Personal Data Protection Framework for coherence and predictability.

2. Appropriate institutional structures should be created to balance these rights in the judicial context. Since judicial functions by courts and tribunals have been exempted from the provisions of the Personal Data Protection Bill, attention must be given to how this gap can be filled. Despite the necessity of such exemption, which enables carrying out of judicial functions independently, specific data protection rights remain a powerful tool to enforce the more general fundamental right to privacy. Therefore, data protection principles must be retained in some form even while courts exercise judicial functions and necessary restrictions and modifications can be made to such data protection principles that take into account the uniqueness of judicial functions. However, unless there is clarity in definitions, standards and approaches within the current set of legislations, formulating a separate data regulation framework for a particular sector, in this case the judiciary, can add another layer of complexity and confusion to the existing contradictions.

3. As far as the access to court records is concerned, as stated before, there is no consensus amongst the courts. As more records have become available via computer networks, there is greater concern about financial information and other personal information contained in such court records being used for fraudulent purposes or to cause harm. Therefore, there is a need to set some indicative tests and guidelines governing access to court records which balances the need for transparency in the workings of the judiciary with privacy concerns of individuals. Access to court records by various stakeholders may be regulated based on their role, function and relationship with the justice system and depending on the sensitivity and granularity of the information sought.

4. The reasons for making court records available (and increasingly electronically) are irrefutable. But there are several approaches that government agencies and court systems can take to minimize the harm to individuals when sensitive personal information is to be posted on the internet while at the same time promoting judicial accountability. Some of the approaches that can be adopted are limiting online access to certain kinds of records while retaining physical access for other kinds of records, adopting access control methods while permitting tiered access

[156] Banisar, David. 2011. The Right to Information and Privacy : Balancing Rights and Managing Conflicts. World Bank Institute governance working paper series; World Bank, Washington, DC.

to court records based on individual's role in the justice system and relationship to the information contained in the court records, adopting practices such as anonymisation and redaction and automating such procedures for particular kinds of personal information that are readily identifiable as such like bank account numbers, driver license numbers, Aadhaar number etc., adopting robust rules and a streamlined access policy, providing judicial data in aggregate form with personal identifying information left out, or by enabling full access under special confidentiality agreements with the court etc.

There is a need to comprehensively examine the public policy objectives of making court records available online. The courts must ask themselves what objectives they are accomplishing by making records available on the Internet, particularly those containing personal information. Would there be a way to limit the amount of personally identifiable information posted on the internet without undermining the purpose of making records accessible? Why are certain types of government records considered public while others are not? Which records need to be public to promote policy objectives such as accountability? Which records should not be released to anyone without the individual's consent? For certain types of records, can public access be limited to just the key elements of the records to achieve transparency? Until the underlying policy objectives are clearly identified, it is advisable to undertake only an incremental approach to posting court records online so that technologies, policies and societal institutions can be allowed to evolve at the appropriate rate to protect privacy while at the same time as promoting the benefits of electronic access.