Paper three

LEGAL FRAMEWORK

September 2019

Whitepaper Series On Next Generation Justice Platform

DAKSH

About the authors

Surya Prakash B.S. is a Fellow and Programme Director, and Leah Verghese is a Research Manager at DAKSH. Amulya Ashwathappa and Siddharth Mandrekar Rao are Research Associates at DAKSH. Madhav Chandavarkar is an independent public policy analyst.

About DAKSH: DAKSH is a Bengaluru-based civil society organisation working on judicial reforms. We are focused on solving the problem of pendency of cases in the Indian legal system. We approach the problem from the perspectives of data, efficiency, process, technology and administration.

This report has been designed by ByTwo Design

September 2019

Acknowledgements

This White Paper is an independent, non-commissioned piece of academic work.

The authors are grateful to Harish Narasappa and Shruthi Naik for their editing contributions, feedback, and comments.

The authors would like to express their gratitude towards Justice (retd.) Madan Lokur, Anil B. Suraj, Bhargavi T.M., Ashwin Mahesh, Poornima Hatti, Rahul Matthan, Sridhar Pabbisetty, Devendra Damle, Pranesh Prakash, Deepika Kinhal, Shreyas Jayasimha, Jacob John, and Gautam John, who participated in a roundtable discussion roundtable discussion on October 17th, 2019, on earlier drafts of the White Papers in this series, including this paper. Their insights, perspectives, and expertise were a valuable contribution to developing the ideas put forth in this series.

Suggested citation:

DAKSH. 2019. *Whitepaper series on Next Generation Justice Platform, Paper 3: Legal Framework.* Bengaluru: DAKSH.

Contents

Paper three

LEGAL FRAMEWORK

DAKSH

Whitepaper Series on
Next Generation Justice Platform

Executive Summary

The path to creating and adopting a citizen-oriented digital public platform for the justice system that meets the principles described in 'Whitepaper Series on Next Generation Justice Platform, Paper 1: Vision' (Paper 1) is determined by two main considerations: the technical requirements necessary to enable it, which are described in 'Whitepaper Series on Next Generation Justice Platform, Paper 2: Implementation and Transition' (Paper 2), and a legal framework to give the justice platform statutory backing, which is the subject of this paper.

While some digital governance initiatives such as the United Kingdom's 'gov.uk' platform have been very ambitious and have had great success in digital service delivery, most of these exclude the judiciary due to concerns of judicial independence. Initiatives to create a digital platform for the judiciary will have to be taken by the judiciary itself. For a change of the scope and magnitude envisaged by the 'Whitepaper Series on Next Generation Justice Platform' to be achieved, there must be statutory backing for overseeing and regulating the process. The best way to achieve this would be through a dedicated law for the creation of the digital justice platform and its regulation.

Such a law will ensure that the design and operation of a platform for the justice system follows well-defined principles at every level including planning, monitoring the progress of implementation, redressing breaches of data, and redressing any harm done to an individual citizen through any misuse or malfunction of the platform. It will help adapt laws and rules on judicial procedure and administration to an online platform, and not require repeated

re-interpretation or amendment of existing laws in these areas.
In addition, the unique context of the judiciary in India means that this law is necessary to ensure that the platform meets its objectives. This is because laws that apply to other branches of government, such as the Information Technology Act, 2000 (IT Act), do not apply to the judiciary. In addition, there are gaps in current laws that govern both the judicial processes and the administration of the judiciary, as well as areas that do not directly concern judicial functions but are relevant to the operation of a platform, such as data privacy. These need to be addressed for the platform to be effective. An overview of the relevant laws and their gaps is given in Chapter 2.

> ***"In addition, there are gaps in current laws that govern both the judicial processes and the administration of the judiciary, as well as areas that do not directly concern judicial functions but are relevant to the operation of a platform, such as data privacy."***

Addressing those gaps could easily be done by amending the specific laws that cover each relevant area where necessary. However, the motivations for adopting a single piece of legislation are driven not only by the vastness and complexity of the laws described in Chapter 2, but also by other factors such as ease of access and comprehension by citizens lacking in legal expertise. Chapter 3 describes the motivations for adopting a legal framework in some more detail and translates those motivations into more concrete objectives for the law itself.

As many countries have moved institutions online, including their judiciaries, there is much that can be learned from their experiences. There is great variation in how extensive their reforms programmes are, as well as in the decisions they have taken regarding which authorities are responsible for the development and administration of their systems, and which branch of government these fall under.

Based on the insights we gain from international experience and the goals that the law should fulfill, we have gained an overview of the potential content of the legal framework in Chapter 3 that would be necessary to realise the vision in Paper 1. These include providing for judicial processes and administration of the judiciary to be done through the platform, protecting the rights of platform users, as well as demarcating the jurisdiction and role of the authorities responsible for creation and administration of the platform.

Chapter 4 looks at the experiences of some of the countries in digitising the judiciary, as well as some of the laws that they changed or introduced to achieve this.

1 Current status

1.1 CURRENT LEGAL PROCESS

Justice is an outcome of process. One of the major reasons that adjudication through the formal legal system is one of the primary means for dispute resolution is that the judiciary follows specified processes that offer a modicum of certainty and fairness and guarantee against arbitrariness. It is for this reason that unconstitutionality is determined not just substantively on the content of a law, but also procedurally and how it is implemented. For the purposes of this paper, the laws dealing with judicial processes have been categorised as follows:

1. Laws on judicial procedure

a. Code of Civil Procedure, 1908 (CPC)

The CPC prescribes procedure for all civil cases. The main body of the CPC contains provisions on pleadings, jurisdiction, execution of orders and decrees, and appeals.

b. Code of Criminal Procedure, 1973 (CrPC)

The CrPC, much like the CPC describes the entire life cycle of a criminal case beginning with the filing of the First Information Report. The CrPC contains provisions related to arrest, bail, investigation and criminal trials.

c. The Indian Evidence Act, 1872

The Indian Evidence Act details what kinds of evidence can be relied upon in a courtroom and how.

2. Rules

High courts have the power to issue rules for judicial procedure within their jurisdiction.[1] The CPC and CrPC both contain provisions enabling high courts to pass such rules.

[1]The authority of high courts to make rules for and prescribe forms for district courts in their jurisdiction is granted by Article 227, Clause 2, Constitution of India, 1950.

Part X of the CPC enables rules to be passed for high courts or district courts that may amend the detailed steps involved in a case as outlined in the First Schedule. However, this power is not unfettered as these rules may only provide for a few items as specified in Section 128 (2) of the CPC, out of which the following items are relevant to justice platforms:

a. The service of summons, notices and other processes by post and the proof of such service;

b. The procedure in suits by way of counterclaim, and the valuation of such suits for the purposes of jurisdiction;

c. Summary procedure;

d. The procedure for originating summons;

e. The consolidation of suits, appeals and other proceedings;

f. Delegation to any Registrar, Prothonotary or Master or other official of the Court of any judicial, quasi-judicial and non-judicial duties; and

g. All forms, registers, books, entries and accounts which may be necessary or desirable for the transaction of the business of civil courts

Section 477 of the CrPC mentions only one matter that high courts can issue rules on - petition-writers, but it does empower the high courts to make rules "for any matter which is required to be, or may be, prescribed". In addition, Section 476 also empowers high courts to prescribe the forms needed to be followed, subject to Article 227. The Supreme Court however derives its authority to issue rules regarding its own procedure from Article 145 of the Constitution of India.

1.2 INFORMATION TECHNOLOGY AND THE JUDICIARY

Section 6 of the Information Technology Act (IT Act) creates an obligation on government authorities to make their filing processes electronic. Though Section 6 is not applicable to the judiciary,[2] limited implementation of E-filing has been conducted in some districts under the E-Courts project. E-filing has many benefits, including an increase in efficiency,[3] a reduction in costs to all parties (of the time, effort and money required with physically filing documents), and as a result, an increase in the use of these records by citizens.[4] However, to give the e-filing process its necessary legal sanction, the appropriate authorities need to pass rules regarding the transition towards a new electronic system. This requires not only careful thought and consideration, but a significant amount of research. It is probably for this reason that the then Chief Justice of India, Hon'ble S. Rajendra Babu, sent a letter to the Ministry of Law and Justice in 2004 requesting that a committee be constituted to assist in the

[2] Section 6, Information Technology Act, 2000. The section only refers to recognition of usage of electronic records and signatures by the 'appropriate Government', meaning the Central Government or any state government.

[3] Gary P. Johnston and David V. Bowen. 2005. 'The benefits of electronic records management systems: a general review of published and some unpublished cases', *Records Management Journal*, 15(3): 131-140.

[4] Shampa Paul. 2007. 'A case study of E-governance initiatives in India', *The International Information & Library Review*, 39(3-4): 176-184.

digitisation of the judiciary.[5] The Union Cabinet approved this request and thus constituted the E-Committee. The e-Committee functions under the aegis of the Supreme Court, with the Chief Justice as the Patron-in-Chief-cum-Ad-hoc Chairman.

The e-Committee published the National Policy and Action Plan for Implementation of Information and Communication Technology in the Indian Judiciary (NPAP) in 2005 after consultation with relevant stakeholders from the judiciary, government, and public.[6] The NPAP divided the implementation of ICT reforms in the judiciary into three phases, and made the E-Committee the apex supervisory body for the process. It also outlined which agencies will be responsible for the implementation of ICT reforms at different levels of the judiciary.

A year later, the Government of India approved the National E-Governance Plan (NEGP) that sought to consolidate the various digitisation efforts of government agencies under a coherent vision.[7] The stated vision of the NEGP is to "make all government services accessible to the common man in his locality, through common service delivery outlets, and ensure efficiency, transparency, and reliability of such services at affordable costs to realise the basic needs of the common man". The NEGP has a three-tiered approach, the first of which is the creation of Common Service Centres which deal with front-end delivery of services to citizens. The second is State Wide Area Networks and State Data Centres which aim to improve the support infrastructure that enables government agencies to share information with each other and citizens. The final tier is Mission Mode Projects, which identify high priority citizen services that need to be transitioned from a manual process to an electronic one. The E-Courts initiative, as envisioned in the NPAP, has been included as one of the 31 Mission Mode Projects.

A common concern regarding E-Governance is the fact that remote access to information opens up possibilities of misuse of personal information. This means that regulation is necessary to protect citizens from harm in the event of misuse of personal data by a third party. An overview of the current status of data protection in India is given below.

1.3 DATA PROTECTION LAW

A significant proportion of human interactions now take place electronically. People's engagement with others on social media and websites and a host of business activities are now conducted electronically. To facilitate easy access to citizens, as well as improve their own efficiency, many government services have shifted to websites and mobile applications. Each of these interactions and transactions generate a wealth of data, that when compiled over time can be used to create very accurate profiles about the individuals involved. These profiles can reveal extremely private information such as their current location, names, gender, sexual orientation and political affiliation. Thus, any process of digitisation must account for data protection to secure the privacy of individuals.

In India, the usage of personal data or information of citizens is regulated by the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (IT Rules) that were passed under Section 43A of the IT Act, 2000 (IT Act). These IT Rules define personal information of an individual as any information which may be used to identify them. In case of any negligence in maintaining security standards while dealing with the data, the IT Rules hold the body corporate (who is using the data) liable for compensating the individual. However, given the limitation

[5] E-Committee, Supreme Court of India. 2005. 'National Policy and Action Plan for Implementation of Information and Communication Technology in the Indian Judiciary'. *E-Courts*. Available at https://districts.ecourts.gov.in/sites/default/files/action-plan-ecourt.pdf. (accessed on 23 August 2019).

[6] E-Committee, Supreme Court of India. 2005. 'National Policy and Action Plan for Implementation of Information and Communication Technology in the Indian Judiciary'.

[7] Ministry of Electronics and Information Technology, Government of India. 2018. 'National e-Governance Plan'. *Ministry of Electronics and Information Technology, Government of India*. Available at https://meity.gov.in/divisions/national-e-governance-plan (accessed on 23 August 2019).

under Section 43A of the IT Act, the IT Rules does not apply to data generated by the government.

In this context, the Supreme Court's unanimous decision upholding privacy as a fundamental right under Article 21 of the Constitution in *Justice K S. Puttaswamy (Retd)* v. *Union of India*[8] will play a pivotal role in determining the extent to which laws must protect data on the platform. The judgment, which emerged from a challenge to the Aadhaar identification system, deals with the usage of data by the state bodies and laid down a test to determine when the State can invade the privacy of its citizens. This test requires the three following conditions to be met:

1. Legality – the invasion must be expressly sanctioned by law;

2. Necessity – the invasion must be in furtherance of achieving a legitimate state aim under the Constitution; and

3. Proportionality – the extent to which the state invades the individual's privacy should be proportionate to the needs for achieving the legitimate aim. This condition is broken up into the following aspects:

   a. Legitimacy of the goal – the specific measure invading the individual's privacy must have a legitimate goal;

   b. Suitability or rationale nexus – the invasion must have a rational nexus with the achievement of the goal;

   c. Necessity – the possibility of another alternative which is less restrictive but equally effective should be ruled out before proceeding with the invasion of individual privacy; and

   d. A positive balance – the cost that the invasion has on the rights of individuals needs to be compared with any of its potential benefits to determine whether there is a net benefit to individuals.

While a data protection law is necessary to protect individuals against breaches and attacks, it needs to be balanced with the dissemination of data on the activities of public institutions which is necessary to ensure democratic accountability. The next section describes the state of open data law in India, showing that change is necessary to create a culture of proactive transparency in government institutions.

> ***"The Constitution of India provides that India is a democratic republic, and a fundamental part of such a system is that the State is ultimately accountable to the public."***

1.4 OPEN DATA LAW

The Constitution of India provides that India is a democratic republic, and a fundamental part of such a system is that the State is ultimately accountable to the public. However, in order to ensure that this accountability is achieved in reality, there need to be channels of information regarding State functions that allow Indian citizens to know how the government is performing.

With the advent of information technology and data analytics, the potential channels of information have increased significantly, leading to discussions on 'open data' policies. The core philosophy of 'open data' is that any information or data collected through the use of public funds should be treated as a public resource that is accessible to all citizens equally and allow the State to use as per law, subject to privacy and security regulations. In the digital age, this

[8] Justice K S. Puttaswamy (Retd) vs Union of India, (2017) 10 SCC 1, 24-08-2017.

should also mean that public institutions design their e-governance platforms in a manner that allows for interoperability between institutions with easy data extraction, and also that any public data be released in machine readable formats.

There are many reasons why an open data policy is crucial and is the need of the hour. Not only can it make the government more transparent and accountable, it can also enable the analysis of government data, by both the government and the citizenry. Such analyses can lead to insights into the functioning of the government that can be used to improve such functioning.[9] There can be various types of open data platforms, which include tools that facilitate real-time interactions, increase public access to government systems, and systems that augment accountability in governance.

Open data and the government

A watershed moment in the history of open data in India took place with the passing of the Right to Information Act, 2005 (RTI Act), which made access to government data a statutory right. Section 4(2) of the RTI Act created an obligation for state agencies to proactively release information to the public. Section 4(2) of the RTI Act then led to the Union Government announcing the National Data Sharing & Accessibility Policy (NDSAP) in 2012,[10] where they also launched the Open Government Data Platform (OGD) to make government datasets publicly available.

[9] Barbara Ubaldi. 2013. 'Open Government Data: Towards Empirical Analysis of Open Government Data Initiatives'. OECD *Working Papers on Public Governance* No. 22. Available at https://www.oecd-ilibrary.org/governance/open-government-data_5k46bj4f03s7-en (accessed on 23 August 2019).

Open data in the judiciary

There is a long track record globally of openness being recognised as an inherent part of the judicial process. Indian law has also followed in these footsteps. Section 327 of the Code of Criminal Procedure, 1908 and Section 153B of the Code of Civil Procedure, 1908 both contain express provisions that declare that courtrooms shall be open to the public. A nine-judge bench of the Supreme Court has also recognised the principle of open courts in *Naresh Shridhar Mirajkar* v. *State of Maharashtra*,[11] though it was caveated with the rule that openness should not come at the expense of justice being administered. Most recently, the Supreme Court furthered the principle of open justice by approving live streaming of court proceedings provided open courts do not impinge upon the cause of administration of justice.[12] Further, in light of its decision in the *Puttaswamy* case, that it should not violate the privacy rights of parties, the Court also held that it would hold the copyright of the recordings.[13]

1.5 FLAWS WITH THE CURRENT SYSTEM OF RECORDING AND ACCESSING JUDICIAL DATA

1. Antiquated systems:

The current laws were designed using a paper-based model that exhibits drastically different properties from a digital-based model. The lack of laws on how data is captured can drastically limit the full potential of a digital platform for the judiciary if the same paper-based processes are merely converted into digital ones. The points below describe the gaps in the current legal environment that need to be addressed in order to implement a justice platform.

[10] Ministry of Science and Technology, Government of India, 2012. 'National Data Sharing and Accessibility Policy'. *Ministry of Science and Technology, Government of India.* Available at https://data.gov.in/sites/default/files/NDSAP.pdf (accessed on 23 August 2019).

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

[12] Swapnil Tripathi v. Supreme Court of India, Writ Petition (Civil) No. 1232 OF 2017.

[13] Section 52(d), Indian Copyright Act, 1957.

a. Possession vs. Control

In a paper based model, court information is kept in paper files located in courthouses within the physical control of the judiciary. Under all the present rules for the Supreme Court, high courts, and district courts, anyone seeking to access court documents has to submit a physical application to the court registry and the registry has the discretion to either allow or refuse access. Possession of court information is thus synonymous with control over it.

b. Document vs. Information

The paper based models currently in place in India use documents as their basic unit – a court file typically comprises a number of documents. However, a court file in a digital based model will contain a large number of information fields that may be sourced from and dispersed across a variety of different locations. For example, a criminal court file will contain fields of information from police, courts, and prisons in various jurisdictions. The primary difference between a paper document and a digital document is that a court file can be considered in much more granular terms by recognising the many separate components of information that reside within it. This enables a judicial system to manage and exchange 'fields of information' rather than capturing the information within paper 'documents'. However, such a system would require a complete overhaul of processes used, both within the judiciary, as well as external interactions with other justice delivery bodies.

c. Lack of data analysis

One of the biggest revolutions that IT has brought to functionality of systems is data analysis. Data analysis can provide in-depth insights into the performance of an organisation and greatly improve efficiency and efficacy. Since judicial processes in India were envisioned in a bygone era, many of the systems of approval for access to court information are tied to individual cases. While the National Judicial Data Grid provides case-level analysis for all district courts and some high courts, there is scope for more granular analysis. This also makes the analysis of judicial performance more difficult without envisioning new procedures, which is a lost opportunity for increasing public trust in courts.

d. Data is not digital by default

Since current digitisation efforts are merely an overlay over the paper-based model, there are many drawbacks in their implementation. To begin with, there is a duplication of work with respect to data entry when paper-based information has to be uploaded digitally. This is then compounded by the fact that many documents and files are merely scanned and uploaded, negating their digital utility as information contained in them is consequently harder to extract. These issues prevent any digitisation efforts from delivering the full range of benefits such as increased efficiency or access. The current efforts of only digitisation should be replaced with digitalisation of processes.

e. Limitations of physicality

Court records can often be extremely voluminous, containing a large number of documents of varying length. This places a physical limitation with respect to storage as not all information can be stored in perpetuity. There is thus a requirement that ancillary documents to a court case are to be destroyed after a certain period, which is a constraint that does not exist in a digital system.

f. Poor accessibility

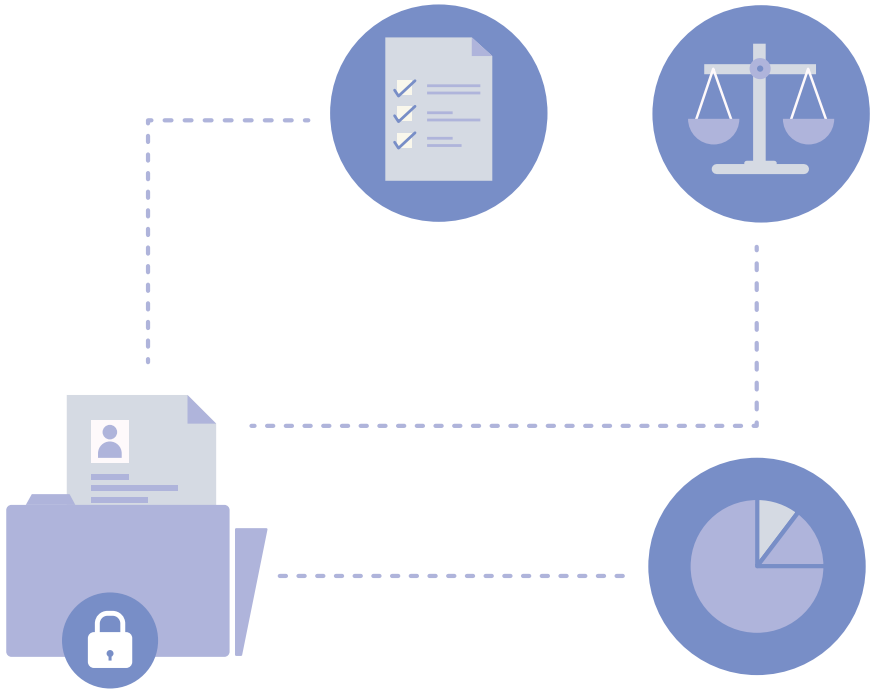
By its nature as a physical document, a paper-based court file provides significant barriers of cost and effort for those who wish to access it. This ensures that only the parties or those involved in the case will go through the lengths necessary to access it, and that is only if they have the means to do so. This precludes access to court information not only to a large section of the public, but, most importantly, to those parties unable to expend the necessary monetary resources and time.

Though the judiciary has made impressive steps to upload judgments,

all websites with such judgments contain legal disclaimers that the court neither guarantees the accuracy, security (with respect to viruses), or validity (in terms of being up-to-date) of any information provided nor indemnifies any party's reliance on the same. This somewhat undercuts the impact of uploading judgments online by rendering them largely referential. Furthermore, judgments are at the tail end of the judicial process - there is a host of court information that is only stored physically and remains digitally inaccessible.

2. Absence of statutory backings of E-committee and privacy/data protection laws:

One of the biggest drawbacks with the current framework for the digitisation of the judiciary is the lack of statutory backing. Though constituted by the Ministry of Law and Justice, the E-Committee is a part of the Supreme Court and reports only to the judiciary. Furthermore, the only document detailing digitisation is the NPAP, which is only a policy and does not qualify as a rule under Article 145. As such, it is not possible to approach the judiciary under Articles 32 or 226 to enforce its implementation. As the E-Committee is the apex agency under the NPAP and responsible for both setting the direction and supervising all digitising efforts, the modernisation of the judiciary into a completely digital institution is entirely reliant on its performance.



It is also the case that fully digitising the judiciary will require amending a compendium of existing procedural laws and data protection laws.

Furthermore, under the *Puttaswamy* judgment, any government collecting personal data of a citizens must pass the 3-fold test of necessity, legality, and proportionality. The first is fairly self-evident with respect to a judicial system, but the test of legality requires that there must be a law empowering the state to handle such information, which does not exist.

3. Difficult for citizens to navigate through the judiciary:

Rules regarding judicial processes are first and foremost, not accessible for average citizens. Even if citizens manage to access them, the processes they create and the language they are written in are often too complex or obscure to follow, and requires citizens to rely on their lawyers to navigate court processes.

The next stage of reforms for the judiciary and its information systems should fill these gaps, using the present systems as a starting point. The strategic and technical approaches needed to achieve this are given in Paper 2, and Chapter 3 of this paper chalks out the need for a legal framework to guide the implementation of the platform.

2 Why do we need a legal framework for the platform?

Creating a legal framework for the justice platform gives both the platform and the authority that governs it a legal backing. The main advantages of having a legal framework is that it enables justiciability of the platform's processes and accountability of the platform authority. The points below detail the reasons as to why we need a legal framework for the platform.

1. To establish an authority who will be responsible for the justice platform

The creation, implementation, administration, and improvement of the platform should be done by a dedicated permanent authority. The legal framework is necessary to set out the terms of the establishment and functions of the authority. The powers of the authority and their limits must be clearly laid out in the law and also to hold the platform authorities accountable. A designated authority can bring in certainty to the implementation of the platform rather than an authority backed by policy. An authority constituted under a policy framework lacks legislative guidance.

In the current political scenario, the judiciary might resist the establishment of a designated authority which has a legislative backing but in an established authority the judiciary would play a leadership role in the implementation of the platform.

2. To make processes justiciable

A core goal of the legal framework is to make features of the platform justiciable, and to provide a means for citizens. The legal framework can also make the provisions of the law, especially those relating to citizens' rights and the obligations of the platform authority, to be fair and reasonable as per constitutional values. In the interest of procedural due process, the legal framework can regulate the processing of a case through the platform to ensure due process is met by digitising it and minimising human interaction and biases. The legal framework can ensure that any deviance from procedural due process through the platform is addressed in the court of law. To meet the current efforts of digitization of judicial process a legal framework becomes a necessity to prevent any procedural irregularity.

3. Consolidation of relevant laws

Many existing laws would need to be amended to make the platform possible. These laws span areas ranging from procedural laws and administrative regulations. Without a single legislation which establishes the platform and the terms of its operation, making these changes would require amendment of every

individual law governing the operation of the judiciary. This means that any future improvements to the platform after its implementation could potentially require amendment of all these laws, once again. Such a process is complex and difficult, therefore a consolidated law for the platform would be ideal.

The legal framework would also serve as a single source of information regarding the platform, its use, its design, the setup of the platform authority, and the accountability mechanisms. Currently, the setup of courts and the rules that govern their operation, and the procedural law that directs the process of litigation, are codified in multiple sources. This makes it difficult for ordinary citizens, who lack legal expertise, to comprehend this information. Even though judges and lawyers are familiar with this information, their work could be simplified if there was a single law governing the operation of the judiciary on the platform.

4. Data protection

Sensitive information is frequently an important part of legal proceedings, even though cases are heard in an open court. The ability to possess, transform, and use information, particularly when done in bulk, could have harmful consequences. There is thus a need to protect the privacy of citizens while observing an open data principle.

Until India adopts a data protection policy at some point in the future, a dedicated legal framework is necessary to provide for adequate data protection for citizens, and for violations of citizens' data rights.

This chapter lays down the need for a legal framework which is necessary to accelerate the digitisation of the Indian judiciary.

3 Legal framework

In this chapter we lay out the essential requirements of a legal framework for the platform. The idea is to encapsulate the broad requirements of the framework that will help realise the vision of having a single platform for the judiciary.

3.1 OVERVIEW OF LEGAL FRAMEWORK

This section provides an overview of the main components of the legal framework for the platform.

1. Core laws and rules:

At the core of the legal framework will be a legislation that defines the platform as the primary location of engagement with the judiciary that does not require physical presence in a court. The core laws will make the features of the platform, and any outcome of their usage justiciable. The citizens will also have legal recourse against any rights violation resulting from the use of any features of the platform or any action taken through it. As key features of the platform fall within the domain of procedural law (such as CPC, CrPC and various high court rules), the core laws will need to link the platform to these laws which will give legal recognition to the performance of any task or judicial service through the platform, where applicable. This will also be the basis for the appointment of authorities to oversee the implementation of the platform, and to run it once implementation is completed. Rules governing the more detailed aspects of the features and usage of the platform are also a key component of the core laws for the platform.

2. Powers and functions of justice platform authorities:

The platform needs to be designed, implemented, and administered by bodies under the oversight of the judiciary. The terms of their establishment and operation must be set out in the legal framework in order to specify their obligations and duties and citizens' rights in relation to them. The legal framework would regulate their activities to give legal backing to the judiciary's authority over all aspects of their functioning, and to ensure that they can be held legally accountable for their activities, including any violations of those regulations.

3. Data protection and disclosure regulations for the justice platform:

As established in Chapter 2, a dedicated data regulation framework is necessary to protect citizens from the abuse of any of their personal information that is stored on the platform and to provide for data on the platform and its administration to be disseminated in the interest of transparency.

3.2 CORE LAWS AND RULES

The core laws that govern the platform have the objectives given below, which can broadly be understood to mean that the law will provide a legal backing for the decision to shift services to the platform, and for the transfer of information to the platform. They will also link with other key legislation, such as procedural law. These laws will be passed at both the Union and State Level.

1. A legal mandate to migrate to the platform

The most essential part of the legal framework for the platform is a law to mandate the use of the platform when citizens come in contact with the judiciary, from the filing of a case to its disposal. The framework should enable the use of the platform and be made the default option for any judicial process. Such a provision will be akin to Section 6 of the IT Act which states that if

> *"The most essential part of the legal framework for the platform is a law to mandate the use of the platform when citizens come in contact with the judiciary, from the filing of a case to its disposal."*

any government agency requires the citizens to submit documents for any government related transaction, such requirement would be complete if the citizens have used such electronic means prescribed.

2. Legitimising key features of the platform

Paper 2 addresses the key modules that are required for a comprehensive online justice platform. The paper prescribes modules such as online dispute resolution, online legal aid, e-filing, case information system, evidence management, summons and notice generation, document management, integration with other systems like the prisons, police, forensic departments, legal databases, etc.

A substantial portion of the legal framework would be dedicated to giving these ICT modules legal recognition as the primary means of performing the tasks they were intended for, and recognising the platform as the primary means for doing so.

3. Transition to the platform

It is essential to lay out the provisions for manual processes and the transition phase, which is defined as the time period during which the existing digital applications are shifted and converted to be hosted on the platform. It includes eliminating applications or projects that run contradictory to the idea of a single platform. Every existing application dealing with some part of a judicial function or connected to the judiciary should be merged with the platform. Existing portals like E-Courts, National Judicial Data Grid, and Inter-operable Criminal Justice System will need to be replaced or adapted to be hosted on the platform. Timelines should be prescribed for eliminating the use of existing applications, for smooth transition.

The framework would also provide the legal basis for the platform authorities to manage the transition from earlier systems to the platform. A chief transitional officer will be appointed under the administrative authority to ensure that existing paper and digital records are converted to a format that can be hosted and easily accessible on the platform.

There are existing services used by the citizens like e-filing, e-payments, and the availability of case information online. These need to be migrated to the platform in a way that does not adversely affect litigants' right to access during the transition phase. Hence, the transitional and the chief guidance officer should ensure that they push users to migrate to the platform by having a support system in place to address all user concerns. More details of the

authorities that will implement and eventually administer the platform is given in section 3.3 of this chapter.

4. Linking to procedural law

Where the features of the platform need to be compliant with procedural laws such as the CPC, CrPC and the Indian Evidence Act, 1872, amendment of those laws may be necessary. The Indian Evidence Act, for example, may need to be amended in order to allow lawyers and judges to remotely view records of evidence through the platform, and regulations could be enacted to ensure that the evidence is documented appropriately and reliably.

5. Rules

The final component of the legal framework for the platform would consist of rules governing the operation and use of the platform. A significant part of this would be criminal and civil rules that are followed in legal proceedings, which are formulated by high courts.[14] These rules would form an integral part of the legal framework for the platform, and high courts could amend them to specify the exact procedures to be followed by platform users over the course of legal proceedings.

The platform rules would give legal backing to all new processes and features introduced, such as online repositories and sharing of evidence, video conferencing, and online submission and scrutiny of documents, among others. Importantly, the rules under this framework would also provide recourse for any violation of the terms of service, and would need to provide for penalties to be imposed and procedures to be followed, to address such a violation.

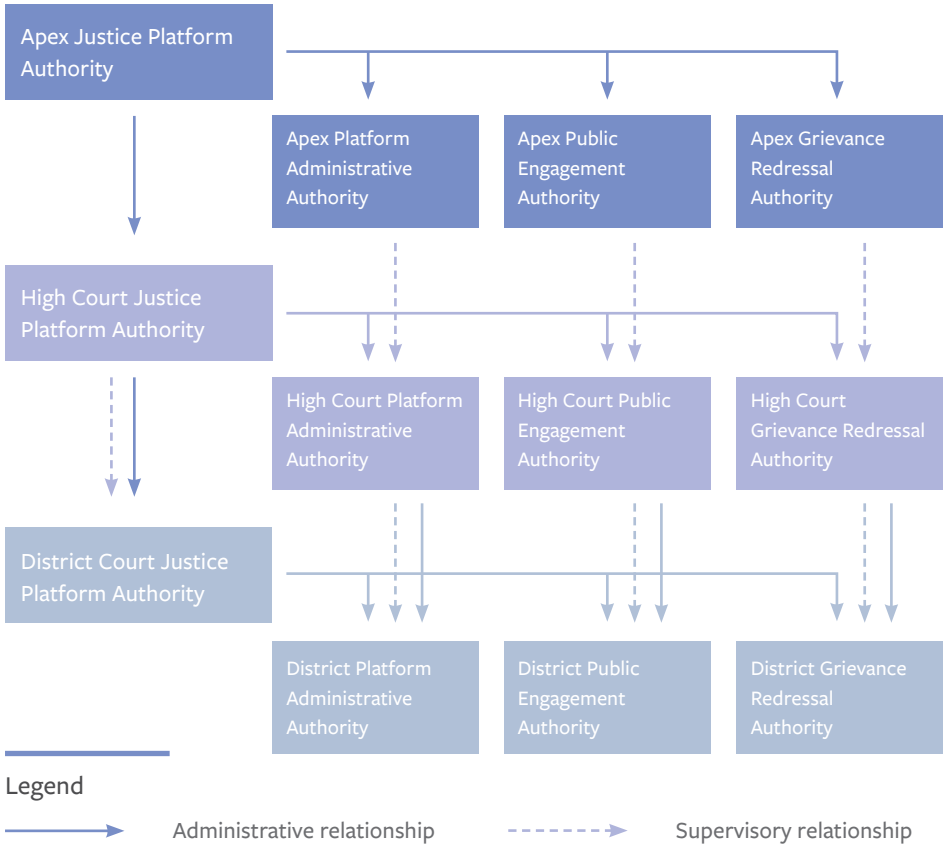
The legal framework would contain a separate set of rules governing the operation of the platform authority itself. This would include details regarding jurisdiction, structure and the sub-authorities within it, the processes it must follow, the division of roles and responsibilities within the authority, and their assignment, among others.

[14] For example, the Andhra Pradesh Civil Rules of Practice and Circular Orders, 1990

3.3 REGULATORY FRAMEWORK FOR JUSTICE PLATFORM AUTHORITIES

The authorities established under this legal framework will have the power to carry out the necessary functions for the implementation of the platform. The justice platform will be implemented and administered using the structural mechanism of Justice Platform Authorities, which shall be present at the level of district courts, high courts and the Supreme Court.

The authorities are as follows:



3.3.1 Apex Justice Platform Authority

The Apex Justice Platform Authority (AJPA) will be the apex authority for the platform. Its primary role will be to supervise and coordinate with the High Court Justice Platform Authorities (HCJPAs) on the implementation and administration of the platform. As the apex authority, the AJPA will also lead the design of the platform so that some homogeneity can be achieved despite individual differences in procedure between states.

The AJPA would predominantly consist of members representing the judiciary, including the Chief Justice of India. Some of these members should have experience or expertise with information technology and public administration, and members representing key bodies within the AJPA, such as the Platform Administrative Authorities (PAA), Public Engagement Authorities (PEA), and Platform Grievance Redressal Authority (PGRA). To ensure that other stakeholder groups' needs are also met, the AJPA will have representation of the Union Ministry for Law and Justice, and the Bar Council of India.

Among its main responsibilities, which will be critical to the platform's early success, is the AJPA's role in driving and guiding the process of adoption of open standards for the platform, as described in Paper 1 and Paper 2. This includes organising and coordinating meetings between stakeholder groups, documenting meetings, accepting submissions of independently research or proposed standards, publication of material such as documentation of meetings, proposals, draft and final standards, organising public engagement sessions and promoting citizen participation, and finally, providing ongoing support to platform users such as maintenance and fixes to keep standards up-to-date.[15]

[15] Ken Krechmer. 1998. The principles of open standards. Standards Engineering, 50(6), pp.1-6.

3.3.2 High Court Justice Platform Authority

The High Court Justice Platform Authorities (HCJPAs) will be the primary authorities for the platform in the jurisdiction of their respective high courts. They will coordinate with the AJPA for the implementation of the platform and monitor all District Court Justice Platform Authorities (DCJPAs) that fall under their jurisdiction. One of the most crucial roles the HCJPAs will play will be in the passing of rules for re-engineered processes necessary to harness the benefits provided by a justice platform, since detailed rules of civil and criminal procedure are often determined at the state-level.

As with the AJPA, the HCJPAs would primarily consist of judicial members representing the relevant high court, and representatives of the state equivalents of the non-judicial bodies and organisations represented in the AJPA. As with the AJPA, each HCJPA would oversee the bodies under its authority and jurisdiction that perform various functions related to the operation of the platform. The HCJPAs would have a degree of independence from the AJPA to allow them to adapt the features of the platform for the differences between how the judiciary operates in different states – for example, differences in procedural laws and rules. They have the responsibility of adapting process re-engineering rules to the state-level laws and rules that have been passed in each state. They would have direct control of the district-level authorities that are responsible for final implementation and operation of the platform, at the level of each district court.

3.3.3 District Court Justice Platform Authority

The District Court Justice Platform Authorities (DCJPAs) will be nodal authorities under the legal framework for the administration of the platform. As such, their primary task will be to coordinate with their respective HCJPAs for the implementation of the platform and monitor the administration and usage of the platform in all courtrooms that fall under its jurisdiction.

Whereas the HCJPAs have relative independence from the AJPA, DCJPAs will be completely under the supervision of the HCJPAs, which will have

jurisdiction over DCJPAs. Given that district courts act as the first point of access for justice for most citizens, the importance of DCJPAs in the implementation of the platform cannot be stressed enough.

It is for this reason that each courtroom shall have one person designated as the Platform Liaison, who will coordinate with his or her respective DCJPA for the implementation of the platform. This Platform Liaison need not necessarily be a new position and existing officers may be designated to perform this function.

The Principal District Judge of a given district would be the President of the DCJPA with representation from the district judiciary, and the DCJPA would oversee sub-structures responsible for the same functions necessary at higher levels, like administration and public engagement. Supervision and assistance of the Platform Liaisons, in order to ensure that the platform meets the needs at the level of each individual court, is a major responsibility of the DCJPAs.

3.3.4 Functions of platform authorities

At each of the three levels described above, the platform authorities must perform certain basic functions necessary to implement and run the platform. They will each have dedicated bodies to perform these functions, though the specific tasks they need to perform will likely vary significantly between each level. The details of these functions and the bodies responsible for them are given below:

1. Administration

Platform Administrative Authorities (PAAs) are bodies tasked with creating and administering the platform in detail. The Apex PAA will directly interface and supervise the performance of the respective High Court PAAs regarding the implementation and administration of the platform. The PAAs will require a team for each of the following functions:

a. Technological development, interfacing with the technology and domain experts to design the platform such that it meets the needs of states, and representing the judiciary at the apex level in the development of open standards for the platform;

b. Budgeting, to determine the budgetary requirements necessary for implementation of the platform within that respective jurisdiction; and allocation of budgetary resources as needed;

c. Training of judicial staff, including both members of the registry as well as judges, in the use of the platform; creating and administering training for this purpose; and

d. Managing the transition to the platform, including migration of court records to the platform. This role will be temporary, as the legal framework will specify a time period by which all existing records will be ported to the platform.

State level PAAs will supervise and assist the district level PAA in the implementation and administration of the platform. They will follow the policies and guidelines laydown by the Apex PAA. They will use the policies to make state specific changes that they require. At district level, the PAA will merely carry out the necessary tasks as prescribed by the State level PAA.

2. Public engagement

The effective performance of the judiciary requires a certain degree of public trust. To secure this trust, Public Engagement Authorities (PEAs) will conduct awareness campaigns amongst the public regarding the platform and its workings. The PEA will coordinate with the respective High Court and District Court PEAs to ensure that the public is made aware of the availability and full functionality of the platform. PEAs will:

a. Publish and analyse data on the platform;

b. Chart out plans to assist external users, particularly during the transition to the platform;

c. Create awareness - At the state level, the High Court PEA will largely function under the guidance of the Apex PEA. They will carry out necessary functions to make the policies translate into actionable steps for the district level PEA. The PEA at the district level will carry out the necessary tasks as prescribed by the High Court PEA.

3. Grievance redressal

Given the critical function a justice platform will play in the dispensation of justice, it is vital that any instances of malfeasance or malfunctioning be suitably addressed. Any grievances regarding the performance of the platform itself, and not of actual adjudication, will be heard before a Platform Grievance Redressal Authority (PGRA) in that respective jurisdiction, at the District, State, or Apex level. Any appeal to a decision of a District Court PGRA will be heard before the High Court PGRA. The Apex PGRA will be the final court of appeal for the grievance redressal mechanism envisaged under this framework.

3.3.5 Powers of platform authorities

The powers of the JPAs would vary according to their level. Broadly speaking, their powers may be as follows:

1. Apex level:

a. The Supreme Court of India will have power to issue directions to the AJPA.
b. AJPA has the power to create rules governing the implementation of the platform on behalf the Supreme Court of India, including procedural laws, which may need ratification by the Parliament. These could form the template for rules passed by the high courts.
c. AJPA has the power to monitor and assist the state-level JPAs in their implementation of the platform.

2. State or high court level:

a. The state-level JPAs have power to make or amend rules governing the use of the platform on behalf of the high courts in whose jurisdiction they are situated, and for the district courts in that state. These may need ratification in the state legislatures depending on the context.
b. They have the authority to monitor, assist, and issue directions to District Court JPAs.

3. District court level:

a. The DCJPAs have the power to issue directions to Platform Liaisons in their jurisdiction. All JPAs have the authority to monitor, assist, and issue directions to the teams responsible for each function, at their respective level.

3.3.6 Provisions for funds, accounts, and audits

For all JPAs, at every level, the legal framework must demarcate the sharing of fiscal responsibilities for these JPAs, and therefore, for the platform. Budgeting for the judiciary and judicial reforms is a much-neglected area,[15] and mapping out the appropriate contributions of the Union and the states is necessary for both the judiciary in general, and for a potential platform, in particular.

The legal framework must ensure that the JPAs have the resources they need to achieve their goals, addressing details such as its funding and borrowing powers. State and Apex level JPAs should prepare and submit budgets and accounts to the appropriate governments and ensure that they are audited by the appropriate authority.

3.4 DATA PROTECTION AND DISCLOSURE REGULATIONS FOR THE JUSTICE PLATFORM

Chapters 1 and 2 established that having a data governance framework for judicial data is an essential component of the platform. We explained that the two primary concerns that this framework needs to address are privacy, to be achieved through data protection; and transparency, to be achieved through open data. The judiciary needs its own dedicated regulations because of the need to observe principles such as open courts.

[15] Centre for Budgeting, Governance, and Accountability (CBGA) and DAKSH. 2018. *Memorandum to the Fifteenth Finance Commission on Budgeting for the Judiciary in India*. CBGA and DAKSH. Available at https://dakshindia.org/wp-content/uploads/2019/06/Memorandum-on-Budgeting-for-Judiciary-in-India-from-CBGA-Website.pdf (accessed on 5 September 2019).

3.4.1 Data protection

Creating a data protection framework for the judiciary and its platform calls for some thought and discussion regarding how existing policies that make sense for physical courtrooms would be inappropriate if simply replicated in the digital context. A key example is the principle of open courts; while citizens are generally free to attend court proceedings, and therefore have access to any information that is read or spoken aloud, an open access digital record of court proceedings would have much greater potential for misuse because of the ease of access. This information can easily be used for malicious purposes such as stalking, profiling, illegal surveillance, or fraud.

Keeping these considerations in mind, a consent-based model of data protection, which is the current norm, is inadequate for judicial data. Rahul Matthan proposes a rights-based model, where consent is not a necessary criterion for processing.[16] In this model, data protection and the legitimacy of data processing are determined by whether the rights given to the subject of the data are protected, and not by whether such subjects have given consent. In a consent model, the subject of the data has the responsibility of ensuring that data use is legitimate, whereas in a rights-based model, this responsibility lies with the data user. Their obligation to observe the data rights of the subject can be legally enforced regardless of whether the subject has given their consent to its use. Since the framework is tailored to the stakeholders of the justice platform, it is based on an understanding of the specific needs, rights, and obligations of each stakeholder group, as both a user and a subject of data.

The data protection framework for the justice platform must differentiate between types of data and the types of stakeholder and their roles as platform users. This determines the applicability of rights and obligations as platform users in the data environment and the level of their vulnerability once their data is disclosed, both of which ultimately form the basis for the level of protection given.

TERMINOLOGY FOR ACTORS IN THE DATA ENVIRONMENT

We follow the Justice Srikrishna Committee's (JSC) terminology for actors in a digital environment.[17] In their report, the key actors are the following:

1. Individuals whose data is collected are 'data principals', and
2. Those who collect this data are 'data fiduciaries'.

In any data protection framework, obligations and restrictions on the activities of data fiduciaries are designed around the needs of the data principal. These activities would include the collection, processing, storage, sharing, accessing, and publication of data.

STAKEHOLDERS GROUPS AND THEIR ROLES, AS PRINCIPLES AND FIDUCIARIES

The justice platform has eight broad groups of stakeholders as described in Chapter 3 of Paper 1. Their needs and tasks as users of the platform vary accordingly. The data protection framework should account for their needs as both principals and fiduciaries.

The stakeholders are the following:

1. Citizens
2. The judiciary
   a. Judges
   b. Court staff
3. Lawyers
4. Police
5. Non-police investigation agencies
6. Public prosecutors and government lawyers
7. Government departments
8. The prison system

[16] Rahul Mathan. 2017. 'Beyond Consent: a New Paradigm for Data Protection'. *The Takshashila Institution*. Available at http://takshashila.org.in/wp-content/uploads/2017/07/TDD-Beyond-Consent-Data-Protection-RM-2017-03.pdf (accessed on 5 September 2019)

[17] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna. 2018. 'A Free and Fair Digital Economy Protecting Privacy, Empowering Indians'. *Ministry of Electronics and Information Technology*, Government of India.

CATEGORISATION OF DATA

Different levels of protection would be required for data depending on the potential harm to the principal if left unprotected; and the role of the data principal, which determines the extent of their rights. All data that is hosted on and used on the justice platform at any point, will be referred to as 'platform data'.

TYPES OF DATA, CATEGORISED BY THE LEVEL OF SENSITIVITY AND PROTECTION

Some data protection frameworks differentiate between levels of data protection granted to data principals based on the level of vulnerability the data disclosure would expose them to. The level of sensitivity of data has a role in determining whether access to it is provided to data fiduciaries besides the principals, and in what form and quantity. We identify three levels of sensitivity and protection, using the same principles, but which would need to be adapted to the judicial context in order to make sense for the platform.

1. Open data

For data in this category, the potential for harm or misuse is negligible. Data such as judgements, orders, pleadings, and cause lists, would be regarded as open data, as would all data which needs to be disclosed for judicial accountability. This category would also contain any other data relating to court cases which does not fit into the other two categories. For any non-open data, the fiduciary would be expected to obtain and demonstrate grounds for processing of the data, which will be described later.

> *"In any data protection framework, obligations and restrictions on the activities of data fiduciaries are designed around the needs of the data principal. These activities would include the collection, processing, storage, sharing, accessing, and publication of data."*

2. Identification data

Identification data is broadly defined as any data which directly or indirectly[18] enables the identification of an individual identity, or which links the identities of individuals with any other information.

Judicial data is unique, in that there are certain types of information which contain personal identifiers that are open access by default, such as judgments and cause lists. These would be classified as open data, as per the rules and principles under which the judiciary operates. Then, the key distinctions between open data and identification data would be in terms of the data protection rights of principals, including the right to be forgotten; and the rights of access. Data principals have no right to demand erasure of judicial data, if it is categorised as open data, especially where its disclosure would

[18] It indirectly enables identification if it can be used to identify individuals if combined or matched with other data possessed by the data fiduciary or which they could be.

be necessary for judicial accountability, or accountability of the government in general. This would be the case, for example, in cases where a government department is a litigant. Any data which identifies individuals, which does not fall under the open data policy, would then be categorised as identification data, usually giving the data principal more control over its use.

The data protection framework should guarantee data principals the right to opt-out from public disclosure of this data, depending on the type of principal, and the source of the data.

If information that can be used to identify individual people has been successfully removed from a dataset, that data can be classified as open data. Data which has been 'anonymised', meaning it has been altered or distorted to make it impossible to identify data principals, meets this condition. However, it is possible that cases where identifiers have simply been stripped or masked can potentially be re-identified, and must be treated as personal data, as per the Justice Srikrishna Committee (JSC) report.

The effectiveness of this category as a basis for data protection has only recently been questioned[19], mainly due to the recent rapid growth in the availability of datasets that can enable indirect identification of individuals when paired with other datasets, which may also be easily available. The JSC report observes that "Data no longer exists in binary states of identifiable or non-identifiable" and attempts to anonymise or de-identify data by removing certain personal characteristics of data principals can fail, depending on the data and the analysis tools available to the fiduciary.[20]

3. Sensitive Case data

In the course of legal proceedings, personal details of people and firms involved in the case are often disclosed. For this reason, legal proceedings are an exception to some data protection laws, in order to maintain independence of the judiciary.[21] The data protection framework for the justice platform should ensure that there are separate, stricter conditions for collecting and processing data of this kind, adapted to the needs of each stakeholder group. For example, the judiciary would need complete access when acting in a judicial capacity, but not when acting in an administrative capacity.

The protection framework should provide for a higher degree of protection for data of this kind, given the greater potential for its misuse. There should be a higher default level of protection for all data that has greater potential for misuse. The requirements for maintaining security of this data should be more stringent, and the penalties for any breach and any further misuse that follows it, should be more severe.

TYPES OF DATA, BY SOURCE

There will be two main sources of data that will be hosted by the platform. The difference between the two is that the first category mainly covers the relationship between platform users and specific cases, and the second covers their relationship with the platform itself.

[19] JSC Report, cites OECD. 2013, 'Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines', OECD Digital Economy Papers, No. 229, *OECD Publishing*, Paris. Available at http://dx.doi.org/10.1787/5k3xz5zmj2mx-en (accessed on 5 September 2019).

[20] The JSC report that it is futile to regulate the standards for anonymisation or de-identification through law due to rapid advancement of technology, and instead recommends that this role is handled by the Data Protection Authority envisioned under their draft law. This role would be performed by the Data Protection Authority within the Platform Authority in the case of the platform legal framework.

[21] For example, Recital (20) (which corresponds to Article 2) of the GDPR explicitly state that the GDPR does not apply to data processed by the judiciary in any member state, in order to maintain independence of the judiciary. An official version of the GDPR which matches recitals with their corresponding articles. Available at http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf (accessed on 5 September 2019). Also see https://ico.org.uk/media/about-the-ico/disclosure-log/2014536/irq0680151-disclosure.pdf for a version of the GDPR arranged such that they can be read side-by-side (accessed on 5 September 2019).

1. Case data (from legal proceedings)

Legal proceedings are the main source of data that will be imported to, stored on, and used through the platform. Data which would be used by the judiciary in a judicial task or by litigants and their lawyers in these roles, for example, would fall in this category.

2. Platform usage and metadata

Data relating to usage of the platform itself, including metadata for services, files, and other resources used, accessed, or shared, covering any action taken by a user of the platform, would form the second category. This would include, for example, the records of usage of services provided on the platform, passwords, and permissions.

The regulations should have different provisions regarding data principals' rights and data fiduciaries' responsibilities for these two categories. This is because the first category must meet different standards of openness, under the same principles currently followed by the judiciary regarding public disclosure of case information. Protections and conditions for third party access for the second category would more closely resemble data protections for use by other branches of government.

TYPE OF DATA, BY QUANTITY AND LEVEL OF DETAIL

The digitisation of processes has made it possible to access detailed data in bulk form, which opens up countless possibilities for third party use. For data generated by legal proceedings, protections and disclosure norms should be formulated based on the following categories, in combination with the others.

1. Case-level data

The case is the basic unit of analysis for any use of judicial data, since the goal of processing judicial data would often be to understand the outcome of a case. It may or may not be necessary to protect information that an individual case generates. Data access regulations should address whether case-level data should be disclosed to a party or the public, and in what usable form it is made available.

a. Case-by-case access

There is a possibility that the processing of case-level data in bulk could violate rights. For example, in the Facebook-Cambridge Analytica issue, public access to the data Cambridge Analytica used to construct profiles was considered by data principals harmless when accessed in isolation (inferred from their having given consent to its use), but the ultimate use of that data in that manner would violate the data rights set out in this framework. In the case of judicial data, simply denying public access to case-level data may not be legal because other laws and principles mandate that the data should be disclosed. For such a situation, the privacy regulations will enable access to that data for only individual cases, and could restrict access to only the principals and certain types of data fiduciary, depending on the context.

b. Bulk access

For other contexts, fiduciaries may have a broader set of usage rights, allowing fiduciaries to obtain access to case-level data from multiple cases. Bulk case-level data can be used to analyse and improve the performance of the platform. The processing of such data supports accountability by enabling citizens to monitor the judiciary and the platform. Also, quantitative research on law is a growing field, and the data generated by the platform would help support it.

While the elements of bulk case-level data could be accessed individually, it is still worthwhile to separate the two categories and enforce regulations based on them. Data protection rules would prohibit or restrict the use of bulk data irrespective of how it was obtained.

2. Aggregates

Aggregate data is quantitative data that has been analysed, and provides information about a larger and more detailed dataset. Aggregate or summary statistics convey or summarise a general characteristic about a case or about sub-groups of cases within the dataset. The summaries of case-level information hosted on NJDG is an example of aggregate data. Summary statistics are useful for the same purposes as the bulk data, namely judicial accountability, platform

improvement, and academic research. It is possible that summary statistics on court cases may contain no identifiers of the data principals for the individual cases. Disclosure of aggregate data, whether proactive or upon request (including RTI applications) is therefore a useful and common way to meet objectives of transparency and accountability while protecting the privacy of individual data principals.

DEVELOPING A DETAILED FRAMEWORK OF PROTECTIONS AND PERMISSIONS

Detailed regulations regarding protection and disclosure of judicial data would need to be formulated and implemented. The Data Protection Authority would be responsible for creating and updating these rules. The rules should be based on a combination of the following:

1. Data categories listed earlier, in terms of the sensitivity, quantity and granularity, and the source of the data;
2. Rights of various categories of principals;
3. Duties of various categories of fiduciaries;

DATA DISCLOSURE NORMS FOR CASE DATA

With regard to disclosure of information regarding court cases, there are three main principles to decide whether or not the case data of a stakeholder is open data.

1. In the interest of transparency, open data is the most desirable option where public disclosure does not infringe principals' rights.
2. Opt-in non-disclosure will be available to principals of certain stakeholder categories, such as litigants and non-litigants, but in the absence of a decision taken by the principal, this data would be disclosed by default, although it can be erased and its processing can be prevented by the principal in the future.
3. Non-disclosure by default will be the policy for certain kinds of data, based on their level of sensitivity and the resulting degree of vulnerability of the principal.

Table 1 provides an easier way to understand potential disclosure norms for case data applicable to case-level data, not aggregates.

Table 1:
Default data protection rights, based on sensitivity and data rights

	Open data	Opt-in non-disclosure	Non-disclosure by default
Identification data	Judges and non-judicial court staff	Litigants and non-litigants (such as witnesses)	NA
Sensitive case data	Government departments, government lawyers and public prosecutors, police, and investigation agencies	NA	Litigants and non-litigants

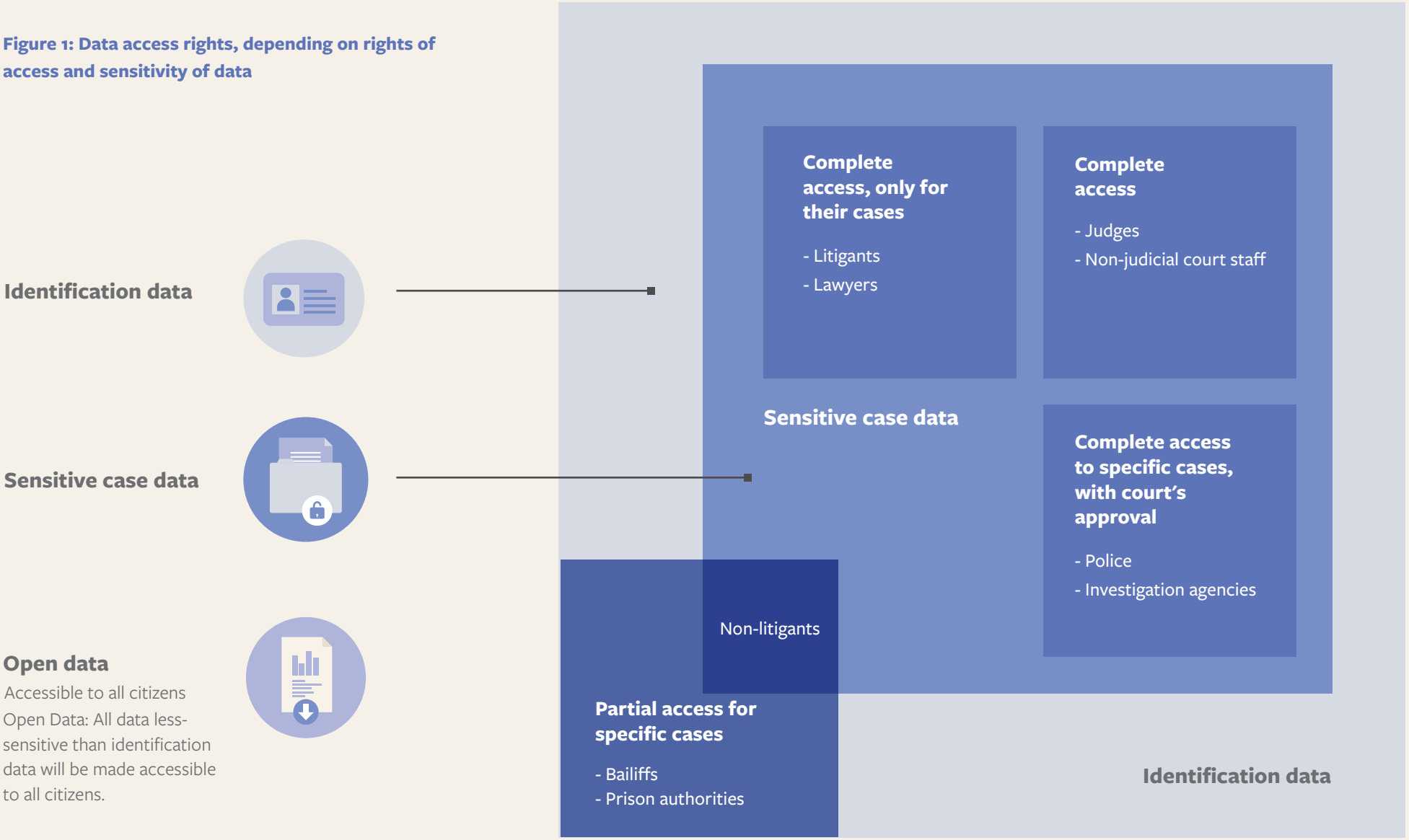
ACCESS NORMS FOR CASE DATA

The permissions to access detailed case-level data in general would also depend on the role of the data fiduciary in a given context. For any non-open data, the fiduciary would be expected to demonstrate grounds for processing of the data. For some stakeholder groups such as litigants and lawyers, this may be only for the cases in which they have these roles.

Where sensitive data is necessary for a fiduciary to perform a legally mandated role, they shall only be granted access to data necessary for and relevant to that role. For example, prison authorities will only have access to the identification data necessary to perform their duties, and would not need access to all the information relating to the legal proceedings themselves.

Figure 2 shows the access rights specific to each stakeholder group, based on its rights, and the sensitivity of the data.

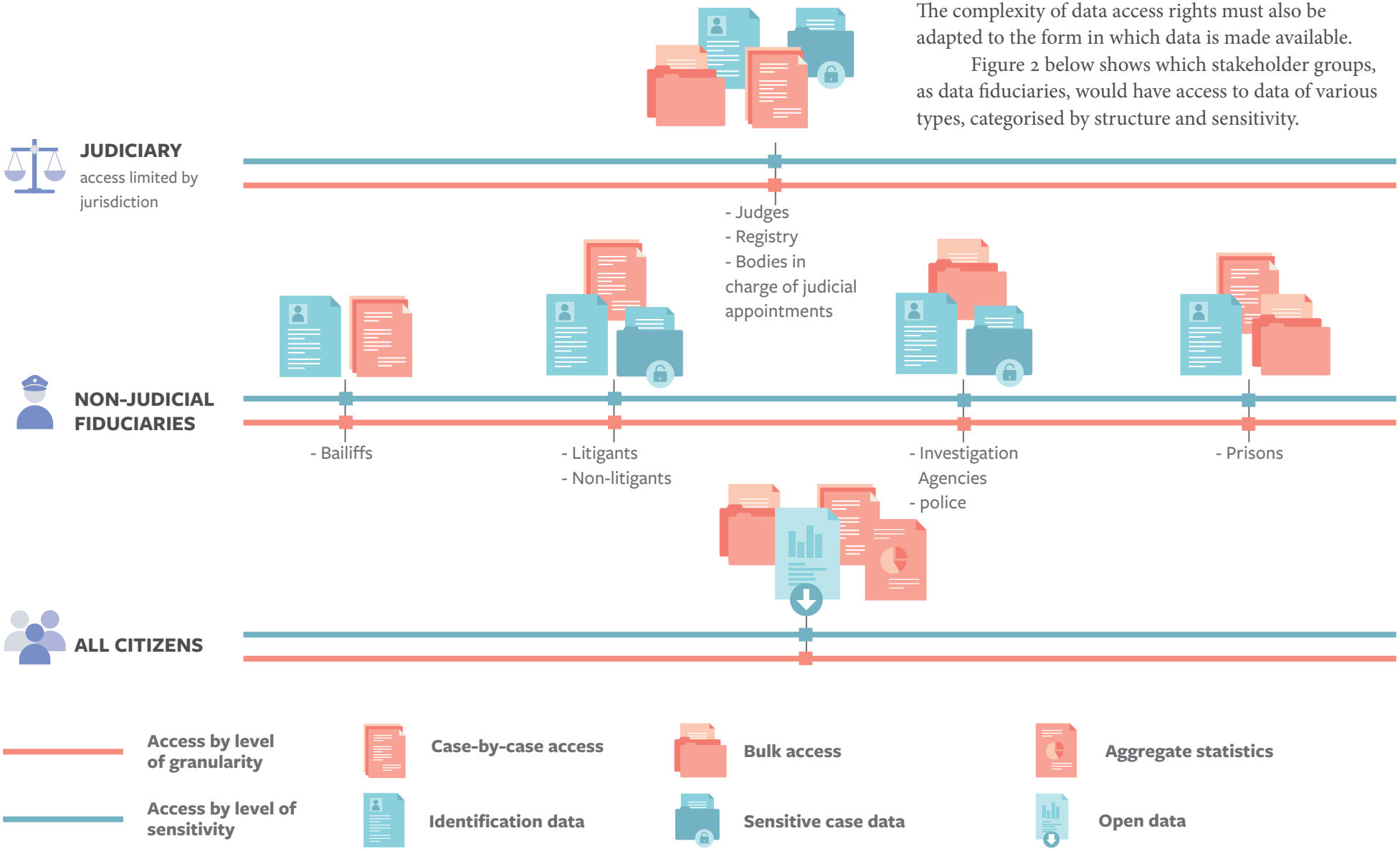
Figure 1: Data access rights, depending on rights of access and sensitivity of data



ADAPTING ACCESS RIGHTS AND PROTECTION RIGHTS TO EACH STAKEHOLDER GROUP

The complexity of data access rights must also be adapted to the form in which data is made available.

Figure 2 below shows which stakeholder groups, as data fiduciaries, would have access to data of various types, categorised by structure and sensitivity.



3.4.2 Rights of principals

Data rights form the core of the protection framework envisioned for this platform. A key distinction should be drawn between how they are applicable to the use of data by the judiciary in a judicial task, and how they are applicable to data use in any other context. It is important to note that not all rights would be available to all principals, or enforceable against all fiduciaries. For example, the right to object to processing and the right to erasure do not apply to citizens as parties to a criminal case. The right to erasure will not be available to government departments..

1. Right to fair treatment

Principals have the right to ensure that any collection, processing, transformation, and sharing of their data, as well as its use in any decision, should be lawful and within the limits of their constitutional rights, including the right to privacy.

Use of judicial data by any fiduciary to make a decision that could impact the lives of the principals should be made fairly and free of bias.[22] This applies to the judiciary and all third parties. Since new technologies are constantly emerging, regulating data use through technology-specific ways is difficult. There is great potential to use data to mislead citizens and influence public opinion, as seen in the Facebook-Cambridge Analytica scandal. Data can also be used as a means to discriminate between people in decisions ranging from employment to the provision of credit.

This right is necessary to ensure fairness in the usage of judicial data even when other rights are harder to enforce. For example, when a principal may choose to publicly share their sensitive case data on the internet, the right to security (see below) becomes much harder to enforce. The principal should still have legal recourse if the data is then misused by some third party.

[22] Mathan, 'Beyond Consent: a New Paradigm for Data Protection'.

2. Right to be notified

The starting point of data protection is the principal's awareness of the collection, storage, and intended use of their data by any data fiduciary. In this case, their rights would be the same for both the judiciary and non-judicial data fiduciaries, including private bodies.

The principal is entitled to know the following:

a. The identity of the fiduciary;
b. Their contact details;
c. Their intended use of the data;
d. The legal basis of the use of their data;
e. The content of the data collected and processed;
f. The data rights of the principal contained in this law, and;
g. Which third parties the data has been shared with by the fiduciary in question.This would be, however, subject to exceptions, such as the data has been given to the fiduciary for the fulfilment of a contract, or the principal having given informed consent.

3. Right to access

The right to access means that the principal will be entitled to be given copies of their identification data or sensitive case data in the form that it has been collected, stored, and processed in.

4. Right to object

Principals have a right to object to the processing of their judicial data. This would, however, only apply to non-judicial use of judicial data pertaining to their court case. This is distinct from the right to erasure (below) in that the fiduciary may store the data, but cannot use it.

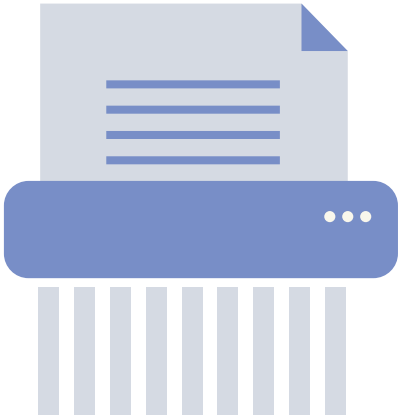
5. Right to security

This right is directly connected to the obligation of fiduciaries to take appropriate measures to ensure the security of their data, explained in the later section on fiduciaries' obligations.

6. Right to erasure and right to be forgotten

Principals can demand the erasure to any data that pertains to them. The 'right to be forgotten' extends beyond erasure; it provides for data principals to request the removal of their personal information from online search results through the deletion of specific kinds of information.

This right also comes with numerous exceptions in the judicial context – such as open judicial data like cause lists or judgements. The applicability of this right would maybe need to be developed by the judiciary itself by setting precedent.[23] A 2017 judgement of the High Court of Karnataka[24] upheld the right to be forgotten in specific contexts, to the extent that the name of the petitioner itself is redacted in some online resources about the judgement.[25]



7. Rights regarding the use of automation in processing data

As they are emerging fields, processes using artificial intelligence (AI) and machine learning (ML) should be approached with caution. Their use should be regulated for most uses, and prohibited for critical ones. As Matthan observes, ML is heavily reliant on patterns inherent in data, and decisions that rely on it have the potential to be discriminatory.[26] There is controversy regarding its use in judicial decisions and sentencing.[27] Principals should therefore have the following rights:

a. The right to object to being the subject of an automated decision;
b. The right to challenge any automated decision;
c. The right to human intervention, which may involve taking the decision independent of any automated process altogether, and;
d. The right against profiling, which has the potential inference of sensitive personal details from a combination of non-sensitive data.

8. Right to accuracy and rectification

Given that judicial data is used to make decisions with serious consequences, it is necessary and fair that principals have a right to ensure that these decisions are made based on accurate data. They have a right to demand that the inaccuracies are duly rectified by the fiduciary.

[23] Rahul Matthan, Manasa Venkataraman, and Ajay Patri. 2018. 'A Data Protection Framework for India'. *The Takshashila Institution*. February 2018. Available at http://takshashila.org.in/wp-content/uploads/2018/02/TPA-Data-Protection-Framework-for-India-RM-MV-AP-2018-01.pdf (accessed on 5 September 2019)

[24] *Sri Vasunathan vs The Registrar General*. W.P. No. 62038 (2016). Available at http://judgmenthck.kar.nic.in/judgmentsdsp/bitstream/123456789/224604/1/WP62038-16-23-01-2017.pdf. (accessed on 5 September 2019)

[25] Sri Vasunathan vs The Registrar General.

[26] Mathan, 'Beyond Consent: a New Paradigm for Data Protection'.

[27] The use of the COMPAS software in judicial decisions in the UK and USA, for example, has been met with controversy over its potential racial bias in estimations of rates of recidivism. There are opposing sides in the debate about whether or not the algorithm was actually prone to bias, but the issue remains unresolved, and automated decision making should be heavily scrutinised and precisely regulated, to protect principals from harm. For more information on COMPAS, see the following:

1. Anupam Chander. 2016. 'The Racist Algorithm?' UC Davis Legal Studies Research Paper No. 498. *Michigan Law Review*, 115:1023. Available at https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1657&context=mlr (accessed on 5 September 2019)
2. Bo Cowgill and Catherine Tucker. 2017. 'Algorithmic bias: A counterfactual perspective. NSF Trustworthy Algorithms.' Available at http://trustworthy-algorithms.org/whitepapers/Bo%20Cowgill.pdf (accessed on 5 September 2019)
3. Anthony Flores, Kristin Bechtel and Christopher Lowenkamp. 2016. 'False Positives, False Negatives, and False Analyses: A Rejoinder to "Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And it's Biased Against Blacks"'. *Federal probation, 80*. Available at https://www.researchgate.net/profile/Christopher_Lowenkamp/publication/306032039_False_Positives_Fals e_Negatives_and_False_Analyses_A_Rejoinder_to_Machine_Bias_There%27s_Software_Used_Across_the_Country_to_Predict_Future_Criminals_And_it%27s_Biased_Against_Blacks/links/57ab619908ae42ba52aedbab/False-Positives-False-Negatives-and-False-Analyses-A-Rejoinder-to-Machine-Bias-Theres-Software-Used-Across- the-Country-to-Predict-Future-Criminals-And-its-Biased-Against-Blacks.pdf (accessed on 5 September 2019)

9. Right to an effective remedy (for violation of the other rights)

This right gives force to the earlier rights, providing for them to be enforced by the appropriate authority.

3.4.3 Obligations of fiduciaries

Data fiduciaries must meet specified obligations in order for their usage of data from the justice platform to be legitimate. These obligations prevent fiduciaries from using platform data in a way that harms principals and violates their rights. While many of these correspond to the rights listed above, they must still be included to give fiduciaries the responsibility for ensuring responsible data use, and a path to do so.

1. Fairness in data use

The fiduciary has an obligation to ensure that their use of the data is lawful and does not violate the principal's rights. Their usage of the data to make any decision impacting the principal's life should also be fair, lawful, and free of bias.

2. Notification of the principal

The fiduciary should proactively provide the principal with the details regarding their use of the principal's platform data.

3. Purpose limitation

Purpose limitation is one of the most important safeguards against misuse of data by a fiduciary. It means that:

a. The fiduciary is obliged to collect platform data only for a specific purpose;
b. The fiduciary must confirm that purpose has a legal basis;[28]
c. It is obliged to confine its use, including processing, to that purpose, and;
d. It may not use the data in any manner incompatible with that purpose.

[28] See below for grounds for data processing

4. Data minimisation

The quantity of data collected and processed should be limited to the amount necessary to achieve the purpose specified. The fiduciary is obliged not to collect more data than is necessary for the purpose of use.

5. Storage limitation

The fiduciary should not store or retain data for a time period longer than is necessary for them to achieve the purpose.

6. Security

The fiduciary bears all responsibility for taking appropriate measures to secure the data of the principal against any loss, modification, breach or misuse that violates their data rights even in cases of accidental technical lapses or of deliberate action by the fiduciary or a third party.

7. Accountability

The fiduciary will demonstrate compliance with the above obligations to the principal. The fiduciary must also have at least one relatively autonomous officer to oversee this compliance, who would be internally and externally accountable for the fiduciary's data processing activities.

3.4.4 Grounds for processing of platform data

The legal basis of the processing of data must be provided for in the judicial data protection framework. Just as not all data protection rights apply to all principals, not all grounds would apply to all fiduciaries, and the framework would need to be detailed enough to account for this. All these conditions would be subject to constitutional and statutory restrictions that apply to the context. Relevant grounds for the processing of platform data are the following:

1. Legal proceedings
The primary grounds for using judicial data would be their use in legal proceedings, by judges, lawyers, litigants, and the registry. This condition is central to the use of the platform.

2. Consent
Despite its limitations, consent, if freely and unambiguously given, fully informed and capable of being withdrawn, constitutes a valid basis for the processing of judicial data, subject to context.

3. Criminal investigation
The necessity of data for a criminal investigation is a condition for processing of platform data. Such data will be available to the police and other investigative agencies.

4. Compliance with orders issued by a court or tribunal
Where the processing of platform data is necessary to comply with an order or judgment by a court or a tribunal, the party to that particular case would process the data as is necessary.

5. Processing is necessary for improvement to the platform
The data generated by the platform is a valuable resource for platform authorities to refine and update the platform. However, the authority would not need access to information about individual platform users, and this condition only allows them to make use of anonymised or aggregated data for this purpose. No other stakeholder group would be able to invoke this condition.

6. Functions of the state
Where data is necessary for sessions of Parliament or state legislatures, it may be processed for that purpose.

7. Contractual obligations
A fiduciary may process platform data if:

a. The processing is necessary for the fulfillment of a contract to which the principal is a party;
b. The processing is necessary for the fiduciary to decide whether to enter a contract with the principal; or
c. The processing is necessary to enter into a contract with the principal.

> *"The fiduciary must also have at least one relatively autonomous officer to oversee this compliance, who would be internally and externally accountable for the fiduciary's data processing activities"*

3.4.5 Transparency - proactive disclosure, open data, and RTI

The data laws for the platform would provide for a framework for the disclosure of data in the interest of transparency and accountability. While proactive

disclosure through the release of open data is an excellent way to foster transparency and to maintain public trust in the platform, it is insufficient to guarantee that citizens have access to all relevant information that they are entitled to. The main reason for this is simply that it would consume too much time and resources for the platform authorities to release all data that should, in principle, be open. The Statistical Office under the AJPA would bear the responsibility of meeting the disclosure requirements set out in the law.

There are three main channels that the Statistical Office would use to disclose data. The first would be proactive disclosure through the form of information prepared by the statistical authority. This is not raw or processed data, but data that has been analysed and interpreted in a way that is easy for citizens to consume, which provides information about litigation in India, as well as information on the performance of the judiciary and the justice platform. This information could be regularly be shared via the platform, and also published as a bulletin or report.

The second channel for transparency would be through the provision of tools for accessing and analysing open data from the platform, covering both case data and platform usage data. In addition to statistical and analytical tools, the platform would provide users with interactive dashboards that easily enable visualisation of this data, much like what is available on the NJDG but which accommodates all the open data that the platform can provide.

Should both of these channels fail to provide information sought by a citizen, the legal framework for the justice platform should be linked with RTI provisons so that citizens can exercise that right as well. Under Section 28 of the RTI Act, The AJPA would be empowered to create rules necessary to appoint appropriate authorities and assign their responsibilities, in order to bring the justice platform under RTI.

3.5 OPEN STANDARDS

As described in Paper 1 and Paper 2, open standards are essential to make the platform work in the manner that it has been envisioned, especially with regard to the flexibility, adaptability, interoperability, and modularity that it needs.

These standards would include the following:

1. Formats for online legal documents,
2. details of entries required to fill out any document or perform any task,
3. file storage formats,
4. Application Programming Interfaces (APIs) to enable communication between modules and the platform,
5. formats for entry of information for internal administration of all institutions (the judiciary, the police, and other stakeholder groups), and
6. formats and procedures for online documentation of evidence, among others.

The standards for the Openness would need to define every aspect of standard setting and adoption except for the fact that the adoption of these standards would be mandated by the legal framework for the platform, once set. The standard needs a legal backing to ensure that it is followed, much like how the formats for legal documents and details of court procedure are backed by rules of high courts and the Supreme Court. As mentioned in section 4.3 of this paper, the AJPA would be responsible for overseeing the standard setting process, including involving stakeholders; and for publication and disclosure of all material relating to standards.

4 International experience

In this chapter we look at Canada, Australia, the UK, and Malaysia to understand their policies on privacy, open data, accessibility and transparency. We also examine the legislation they passed to digitise courts, wherever such legislation exists. From international experience, some of the successful implementation strategies that one needs to focus on, are bootstrapping through simplicity, accessibility, and modularization of the system:[29]

First, the platform should be made simple, easily accessible, and understandable without compromising its 'functionalities, value, usefulness, and legal validity of a procedure'.[30]

Second, implementation should be phased over a period of time to assess each stage of implementation and to gradually move on to the next stage.

While implementing the platform, it is imperative to first select simple procedures that can be digitised and automated, and then have an offline option for complicated procedures and set a time period for the implementation of these selected features.[31] A problem that has caused many countries to abandon their digital courts project is their lack of a clear policy on how to shift from paper to an online platform. In British Columbia, to limit the use of paper, a 'print on demand' rule was established that requires a special request from the judge and other court users to receive e-filed documents on paper.[32] In Australia, at the Federal Court level, the courts with the help of the Chief Justice and the CEO of the courts started an electronic court file system (Digital Continuity 2020), which focused on eliminating the use of paper.[33]

[29] Giampiero Lupo and Jane Bailey. 2014. 'Designing and Implementing e-Justice Systems: Some Lessons Learned from EU and Canadian Examples', *Open Access Journal*, 3(2): 1-35.

[30] Lupo and Bailey. 'Designing and Implementing e-Justice Systems: Some Lessons Learned from EU and Canadian Examples'.

[31] Marco Velicogna. 2007. 'Justice systems and ICT what can be learned from Europe?' *Utrecht Law Review*, 3(1): 129-147.

[32] Heike P. Gramckow, , Erica Bosio, Silva Mendez and Jorge Luis. 2013. 'Good practices for Courts: Helpful Elements for Good Court Performance and the World Bank's Quality of Judicial Process Indicators'. *World Bank*. Available at http://documents.worldbank.org/curated/en/465991473859097902/pdf/108234-WP-GoodPracticesforCourtsReport-PUBLIC-ABSTRACT-EMAILED.pdf (accessed on 16 July 2019).

[33] Federal Court of Australia. 2015. Case study documenting a transition to electronic case files. Available at http://www.naa.gov.au/information-management/digital-transition-and-digital-continuity/digital-excellenceawards/federal-court-of-australia.aspx (accessed 16 July 2019).

4.1 UNITED KINGDOM

The UK began an ambitious programme to modernise the judiciary of England and Wales in 2016, with the goal of institutional transformation through digitisation and the elimination or replacement of inefficient paper-based processes. The movement of key services online has been a part of this, as has a redesign of the internal processes within the justice system. This not only includes the judiciary, but other institutions as well, such as the police and prison services.

AUTHORITY AND RESPONSIBILITY

The UK's reform programme is conducted by Her Majesty's Courts and Tribunals Service (HMCTS).[34] HMCTS is an agency of the UK's Ministry of Justice, and is therefore a part of the executive branch of government. It is subject to joint oversight by the Lord Chief Justice of the Courts and Tribunals, and the Lord Chancellor. The Lord Chief Justice is the president of courts and tribunals in England and Wales, and is responsible for protecting the interests of the judiciary, overseeing training, and representing the judiciary and its views to the legislature and the executive branches. The Lord Chancellor is the minister responsible to parliament for the judiciary. HMCTS is responsible for supporting the judiciary in the administration of justice, allowing the judiciary to focus on its main tasks.

LEGAL BACKGROUND

HMCTS' role and responsibilities have been set out in a framework document,[35] the latest version of which was adopted in 2014. There is no specific legislation that establishes the agency and demarcates its responsibilities – this is done in the framework document, which is subject to parliamentary scrutiny. Any change to the document must be laid before the UK parliament, as must any decision to terminate the agreement.

HMCTS is duty-bound to respond to parliamentary questions. The Chief Executive and the Permanent Secretary of HMCTS are required to appear before the Parliamentary Committee for Public Accounts, when asked to. Additionally, HMCTS' administrative work is within the jurisdiction of the UK's Parliamentary Commissioner for Administration.

LEGAL FRAMEWORK – LEGAL BASIS FOR AUTHORITY

HMCTS follows a set of reform goals set out in 2016 by the Lord Chancellor and the Lord Chief Justice.[36] There is no overarching legislation that defines the reforms that HMCTS has undertaken, or that defines its responsibilities to undertake reforms. It is not a statutory authority and and its reforms programme does not have a statutory basis.

PROCEDURAL LAW

The UK has separate procedural rules for civil, criminal, and family courts. UK procedural law is supplemented by 'practice directions' which are minor procedural regulations.[37] Numerous changes have been made by the practice directions to the civil procedure rules for judicial services to be provided online. For example, practice directions have been created not only for the adoption, but even the piloting of online services.

The UK began rollout of a digital case management system for criminal cases in 2016, following successful pilot projects. The system operates in

[34] HMCTS. 2014. Framework Document. HMCTS Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/384922/hmc ts-framework-document-2014.pdf (accessed on 16July 2019).

[35] HMCTS Framework Document.

[36] Lord Chancellor, the Lord Chief Justice and the Senior President of Tribunals. 2016. 'Transforming Our Justice System'. *Ministry of Justice (UK)*. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/553261/joint -vision-statement.pdf (accessed on 16 July 2019).

[37] MMinistry of Justice (UK). 2017. 'Notes on Practice Directions'. Ministry of Justice. Updated January 2017. Available at https://www.justice.gov.uk/courts/procedure-rules/civil/rules/raprnotes (accessed on 16 July 2019).

Crown Courts, which are the courts of first instance for serious offences (akin to sessions courts in India) and courts of appeal for less-serious offences.[38] As an example of the amendments made to adapt to digital systems, beginning in 2016, the practice directions to the criminal procedure rules have been amended to enable processes and tasks to be conducted primarily through this system, for specific stages of the trial process.[39]

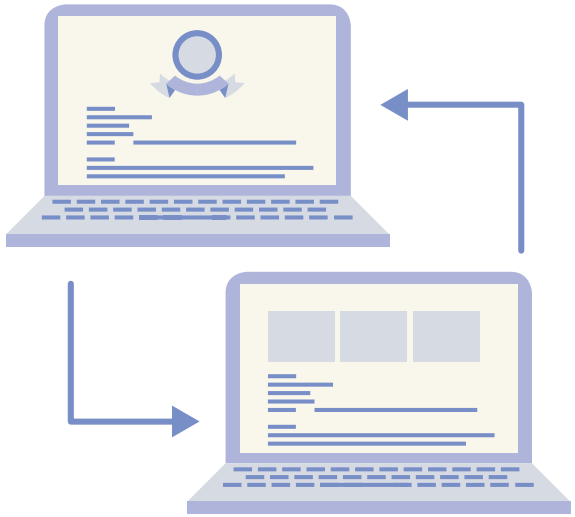
OPEN DATA

Aggregate statistics on the performance of the UK judiciary[40] and court decisions[41] are both published online. For transparency and accountability, the disclosure of data is enabled by the UK's Freedom of Information Act 2000. Court records are exempted under it, and the judiciary is not obligated to release them. HMCTS does, however, fall under the Freedom of Information Act, and discloses details of its releases.[42]

DATA EXCHANGE STANDARDS

For the numerous bodies within the Criminal Justice System (CJS) of England and Wales, there are data standards which prescribe the format for different types of data to be recorded in.[43] They also contain standards for the description of the structure of an organisation, based on the division of responsibilities.[44]

These standards have been published under the UK government's open standards principles.[45] This enables multiple organisations within the CJS to easily share criminal justice information with each other via Information and Communication Technology (ICT).



ACCESSIBILITY

The HMCTS section of gov.uk and the UK judiciary website are the main points of access to judicial services in the UK. HMCTS services are hosted on the UK government's portal, gov.uk. providing services digitally facilitates accessibility. One of the main benefits of a digital medium is flexibility. gov.uk is required to meet accessibility criteria including screen reader compatibility, and provides for users to request content in other formats, such as braille. The judiciary website is optimised for accessibility, being compliant with Web Content Accessibility Guidelines (WCAG) 1.0 level AA.[46] In cases where downloadable files are not friendly for accessibility software, there are provisions for users to request these documents in an accessible format.

[38] Legal Aid Agency. 2015. 'Crime news: national rollout for Crown Court Digital Case System'. *Her Majesty's Government (UK)*. Available at https://www.gov.uk/government/news/crime-news-national-rollout-for-crown-court-digital-case-system (accessed on 16 July 2019).

[39] For example, serving an indictment is done primarily through the system, for which the practice directions were amended in November 2016. See 'Criminal Practice Directions – October 2015' as amended April 2015 & November 2016'. Available at https://webarchive.nationalarchives.gov.uk/20171010144459/http://www.justice.gov.uk/courts/procedure- rules/criminal/practice-direction/2015/crim-practice-directions-II-preliminary-proceedings-2015.pdf (accessed on 16 July 2019).

[40] Ministry of Justice (UK). 'Statistics at MOJ'. *Ministry of Justice*. Available at https://www.gov.uk/government/organisations/ministry- of-justice/about/statistics (accessed on 16 July 2019)

[41] Courts and Tribunals Judiciary. 'Judgements'. *Courts and Tribunals Judiciary*. Available at https://www.judiciary.uk/judgments/ (accessed on 16July 2019).

[42] HMCTS. 2019. 'HMCTS FOI Releases 2019'. *HMCTS*. Available at https://www.gov.uk/government/publications/hmcts-foireleases-2019 (accessed on 16 July 2019).

[43] Ministry of Justice (UK). 2014. 'Criminal justice system: data standards forum guidance'. *Ministry of Justice*. Updated April 2019. Available at https://www.gov.uk/guidance/criminal-justice-system-data-standards-forum-guidance#cjs-standardsand-open-standards (accessed on 16 July 2019).

[44] Ministry of Justice (UK) 2014. 'Criminal justice system: data standards forum guidance'.

[45] Cabinet Office (UK). 2015. 'Open Standards principles' Updated April 2018. *gov.uk*. Available at https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles (accessed on 16 July 2019).

[46] Courts and Tribunals Judiciary. 'Judgements'. *Courts and Tribunals Judiciary (UK)*. Available at https://www.judiciary.uk/judgments/ (accessed on 16 July 2019).

MANAGING TRANSITIONS

For users who do not use digital services or who struggle to do so, HMCTS offers 'Assisted Digital' services, whereby online services are augmented by live assistance from dedicated employees.[47] Crucially, Assisted Digital services aim to support users to use digital services rather than providing paper as an alternative, although paper has not been eliminated in the case of HMCTS.[48]

HMCTS holds periodical events to interact with and gain feedback from users regarding the new services.[49] Despite having formulated a strategy to engage with external stakeholders,[50] it has been criticised for insufficient engagement with stakeholders, especially with regard to digital exclusion[51], the impacts on low-income groups,[52] and the proposed reduction in the role of lawyers under new systems.

The reforms programmes have received much criticism for failure to meet deadlines on their projects, despite being allotted large budgets.[53] The closure of courtrooms under the reforms programme has also received criticism[54] for contributing to the exclusion of low-income stakeholders. Additionally, large-scale failures of their digital infrastructure call the reliability of the system into question.[55]

4.2 AUSTRALIA

In Australia, each state has its own e-courts system set up by the state judiciary. Each state is at a different level of digitisation of the courts but when it comes to policy on privacy, accessibility, open data, and transparency, these states have a uniform policy.

"In Australia, each state has its own e-courts system set up by the state judiciary. Each state is at a different level of digitisation of the courts but when it comes to policy on privacy, accessibility, open data, and transparency, these states have a uniform policy."

[47] Assisted digital and digital take-up community. 2016. 'Designing assisted digital support'. *gov.uk*. Updated July 2018. Available at https://www.gov.uk/service-manual/helping-people-to-use-your-service/designing-assisted-digital (accessed on 16 July 2019)

[48] Mike Brazier. 2018. 'Helping people to use online services'. Inside HMCTS. *HMCTS*. Available at https://insidehmcts.blog.gov.uk/2018/06/28/helping-people-to-use-online-services/ (accessed on 16 July 2019).

[49] HMCTS. 2018. 'HMCTS reform events programme'. Updates July 2019. *HMCTS*. Available at https://www.gov.uk/guidance/hmcts-reform-events-programme (accessed on 16 July 2019).

[50] HMCTS. 2018. 'Engaging with our external stakeholders'. HMCTS. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759859/HMCTS060_ExternalStakeEngageApproach_FINAL.pdf (accessed on 17 July 2019).

[51] Law Society of England and Wales. 2019. 'Written evidence from The Law Society (CTS0040)' (regarding Court and Tribunals Reforms Inquiry). parliament.uk. Available at http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/justice-committee/hmcts- court-and-tribunal-reforms/written/97774.html (accessed on 17 July 2019).

[52] Law Society of England and Wales. 2019. 'Written evidence from The Law Society (CTS0040)'

[53] Financial Times. 2018. 'Court modernisation project risks missing 2023 deadline', *Financial Times*, May 8. Available at https://www.ft.com/content/1e1542c2-4f93-11e8-9471-a083af05aea7

[54] Wen Bowcott and Pamela Duncan. 2019. 'Half of magistrates courts in England and Wales closed since 2010. *The Guardian*. 27 January. https://www.theguardian.com/law/2019/jan/27/half-of-magistrates-courts-in- england-and-wales-closed-since-tories-elected, and Law Society of England and Wales. 2019. 'Written evidence from The Law Society (CTS0040)'

[55] Owen Bowcott. 2019. 'Law courts in chaos as IT meltdown disrupts thousands of cases'. *The Guardian*, 23 January. Available at https://www.theguardian.com/law/2019/jan/23/law-courts-in-chaos-as-it-meltdown-disrupts-thousands-of-cases (accessed on 17 July 2019).

LEGAL BACKGROUND

The Courts Administration Legislation Amendment Act 2016, brought all the federal courts under one authority.[56] Each state has a court administration authority which is established by a state act. For example, Southern Australia has a Court Administrative Authority, and this body is independent of the government which oversees the implementation of technological advancements in the judiciary.[57]

Australia has a digital transformation agency, which is an executive body established under the Prime Minister's cabinet to create public services that are 'simple, clear, faster and customer- centric'. This body is working on providing completely digitised government services.[58] The Federal Courts are also following the footsteps of this agency and their agendas are in alignment with the digital transformation agency.[59]

OPEN DATA

Since court records are excluded from public disclosure under the Freedom of Information Act, open, unmodified data with granular information that can be used for a variety of analysis is not available. At the federal level, data.gov.au provides data sets that are published by various government agencies which capture data in a reusable format.[60]

The court authorities at the federal level on the other hand release annual reports, which talks about the annual court performance and workload statistics.[61] At the state level, the court authorities from time to time release reports which have statistics on judicial data. For example, Southern Australia releases performance statistics report for civil and criminal cases, which provides for clearance rate, lodgement stages, pendency, etc.[62]

ACCESSIBILITY

The Federal Court websites are designed to comply with the Web Content Accessibility Guidelines version 2.0.[63] The websites can also be accessed through assistive technology for differently abled people and the judgments are available on court websites in PDF.

4. CANADA - ONTARIO AND BRITISH COLUMBIA

Ontario has tried two digitisation initiatives of the judiciary, but both of them were unsuccessful. The system aimed at having a simple design and easy information flow but it lacked proper vision for execution.[64] The failure of the systems was attributed to the lack of communication between the government and the vendor. One of main drawbacks was that there were no guiding principles to help realise the vision. The government failed to communicate the vision they envisaged to the vendor, when the vendor was in fact unaware of government's expectations.

[56] Courts Administration Legislation Amendment Act 2016. *Australia Government Federal Register of Legislation*. Available at https://www.legislation.gov.au/Details/C2016A00024 (accessed on 16 July 2019).

[57] Court Administrative Authority of Southern Australia. 'Strategic plan'. *Southern Australia Courts*. Available at http://www.courts.sa.gov.au/OurCourts/CourtsAdministrationAuthority/Pages/default.aspx (accessed on 16 July 2019).

[58] Australian Government, Digital Transformation agency. 'About us'. *Australian Government, Digital Transformation agency*. Available at https://www.dta.gov.au/about-us (accessed on 16 July 2019).

[59] FFederal Australian Courts. 'Corporate plan (2018-19)'. *Federal Australian Courts*. Available at https://www.fedcourt.gov.au/__data/assets/pdf_file/0007/51892/Corporate-Plan-2018-19.pdf (accessed on 16 July 2019 2019).

[60] Australian Government. 'About'. *Australian Government*. Available at https://data.gov.au/ (accessed on 16 July 2019).

[61] Federal Courts Australia. 'Annual Reports'. *Federal Courts Australia*. Available at https://www.fedcourt.gov.au/digital-law-library/annual-reports (accessed on 16 July 2019)

[62] Southern Australia Courts. 'Court performance statistics'. *Southern Australia Courts*. Available at http://www.courts.sa.gov.au/OurCourts/CourtsAdministrationAuthority/statistics/Pages/Court-Performance- Statistics.aspx (accessed on 16 July 2019).

[63] Federal Courts Australia. 'Accessibility'. *Federal Courts Australia*. Available at https://www.fedcourt.gov.au/accessibility (accessed on 16 July 2019);

Southern Australia Courts. 'Accessibility'. *Southern Australia Courts*. Available at http://www.courts.sa.gov.au/Information/Pages/siteaccessibility.aspx (accessed on 16 July 2019).

[64] National Post. 2014. 'Ontario admits it blew $4.5-million on failed court modernization project'. *National Post*, September 19. Available at https://nationalpost.com/news/canada/ontario-admits-it-blew-4-5-million-on-failed-court-modernization-project. (accessed on 16 July 2019).

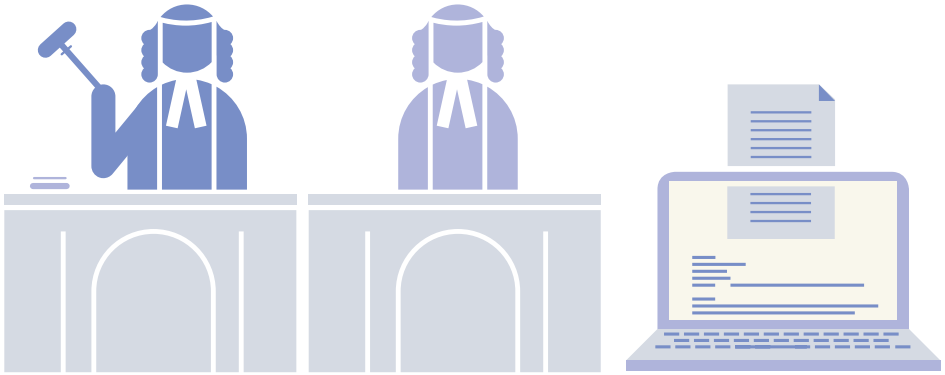
In contrast to Ontario's attempt to digitise their court system, British Columbia has partially succeeded in digitising their court system.[65] British Columbia was able to meticulously plan and execute the implementation by phasing out the adaptation process. It began with introducing JUSTIN, which focused on providing a platform for criminal cases.[66] Once that was completed, it moved to digitise civil as well as family cases.[67] British Columbia's e-courts system has been highly praised for its ability to adapt and modularise the existing system.

LEGAL BACKGROUND

Canada initiated their digitisation of courts in 1996. There are two levels of bodies responsible for digitisation of courts, one at the federal level and the other at the provincial level. Canada has 11 provinces and their ministries of law and attorney generals are responsible to oversee the implementation of digitisation of court system with the help of the Chief Justices of the respective courts.

An administrative service authority has been set up under the Courts Administration Service Act for the federal courts to ensure the judiciary's independence is not compromised by keeping it at an arm's length from the government.[68] The Court Administration Authority's role is to manage human resources, upgrade e-courts, and make any technological changes that are required.[69]

In Ontario, the digitisation of courts is carried out by the Attorney General on the advice of the Chief Justice of Ontario. The Attorney General is



responsible for budgeting and overseeing the implementation of the digitisation process. A Judicial Information Technology Office is responsible to advise the court on information technology and telecommunications services.[70] The Judicial Information Technology Office also coordinates between the Office of the Chief Justice and vendors for the development of multi-year strategic technology plans, to meet the operational needs of the judiciary.[71]

In British Columbia the digitization of the judiciary is overseen by the Chief Judge of the Provincial Courts who ensures that the court service branch of the court carries out the necessary technical tasks.[72]

For the Provincial Court a working group of judges was constituted by the Chief Judge of the court to review the utility and desired technological features to aid judicial officers in the performance of their duties.[73]

[65] The B.C Attorney General put a call out for a vendor for a plan on 'Court Digital Transformation Strategy' and stated that the Court digital system is not up to date with the modern technological advancement. See Kristen Robinson. 2019. 'B.C. Attorney General looking to use digital technology to improve access to justice', Global News, 3 June 2019. Available at https://globalnews.ca/news/5347134/bc-attorney-general-digital-court-update/ (accessed on 16 July 2019).

[66] Jane Bailey. 2012. 'Digitization of Court processes in Canada', Cyber Justice laboratory, *Onatrio and BC study*. Available at https://www.cyberjustice.ca/files/sites/102/WP002_CanadaDigitizationOfCourtProcesses20121023.pdf. (accessed on 16 July 2019).

[67] Bailey.'Digitization of Court processes in Canada'.

[68] Court Administrations Service Authority. 'Role and Mandate'. *Court Administrations Service Authority*. Available at http://www.cas-satj.gc.ca/en/about/mandate.shtml; (accessed on 16 July 2019).

[69] Court Administrations Service Authority. 'Role and Mandate'.

[70] Ontario Court of Justice. 'Memorandum of understanding'. *Ontario Court of Justice*. Available at http://www.ontariocourts.ca/ocj/memorandum-of-understanding/. (accessed on 16 July 2019).

[71] Ontario Court of Justice. 'Memorandum of understanding'.

[72] Provincial Court of British Columbia. 'Annual report 2017-2018'. *Provincial Court of British Columbia*. Available at https://www.provincialcourt.bc.ca/downloads/pdf/AnnualReport2017-2018.pdf (accessed on 16 July 2019).

[73] Provincial Court of British Columbia. 'Annual report 2017-2018'.

OPEN DATA

A harmonious reading of the Privacy Act and Freedom of Information Act mandates the government agencies to disclose the data collected and make it public to increase transparency and accountability of government agencies, though there is no explicit legislative policy on open data.[74] An action plan policy was first released in 2011 by the Canadian government and since then every two years an action plan is released to govern open data norms.[75] The policy broadly follows the eight guiding principles set out by internationally accepted standards of OECD - that the data should be collected by fair means, data should be complete and accurate, the purpose of use should be specified at the time of collection, such collected data should not be used for other purposes, should have safety measures in place to protect the data, general openness of data, individuals should be aware of the data store and inform citizens on how to access it and challenge any restrictions imposed on accessing it, and a data controller should be held accountable for violating any of the principles.[76] A multi-stakeholder forum on open government is set up which comprises eight civil society members and four government officials to facilitate dialogue between Canadian citizens and the government.[77]

Each of the courts at the federal and province level have released yearly or half-yearly reports. The courts of Ontario have statistical reports released yearly of criminal courts, family courts, provincial court offences and bail.[78] The courts of British Columbia have half yearly reports on the time taken to complete trial and general annual reports.[79]

ACCESS TO COURT RECORDS

Canada is a bi-lingual state and case information and other case related information is available in English and French on the court websites. Ontario only provides cause lists online, while British Columbia provides the case status and case history details.

The website of the Supreme Court of Canada makes available information in a user friendly and simplified form. The website has case summaries for ongoing cases and the memorandum of arguments of parties, excluding personal information.[80]

[74] Geothink, 'Citizens guide to open data'. Open data and privacy. *Geothink*. Available at https://citizens-guide-open-data.github.io/ (accessed on 16 July 2019)

[75] Government of Canada. 2018 -2019. 'National Action plan'. *Government of Canada*. Available at https://open.canada.ca/en/content/canadas-2018-2020-national-action-plan-open-government#toc3-5. (accessed on 16 July 2019).

[76] Government of Canada. 'Open Data Principles'. *Government of Canada*. Available at https://open.canada.ca/en/open-data-principles.(accessed on 16 July 2019).

[77] Government of Canada, 'Multi Stakeholder forum'. *Government of Canada*. Available at https://open.canada.ca/en/multi-stakeholder-forum-open-government (accessed on 16 July 2019).

[78] Ontario Court of Justice. 'Court Statistics'. *Ontario Court of Justice*. Available at http://www.ontariocourts.ca/ocj/statistics/ (accessed on 16 July 2019).

[79] Provincial Court of British Columbia. 'Court Reports'. *Provincial Court of British Columbia*. Available at https://www.provincialcourt.bc.ca/news-reports/courtreports (accessed on 16 July 2019).

[80] Supreme Court of Canada. 'Case information'. *Supreme Court of Canada*. Available at https://www.scc-csc.ca/case-dossier/cb/index- eng.aspx. (accessed on 16 July 2019).

4.4 MALAYSIA

The Malaysian court digitisation programme (E-Courts) aims to develop a purely digital information system for the Malaysian judiciary. Following successful pilot projects, its rollout began in 2011, with the main goal of creating paperless 'green courts'. The system has key services online, such as filing of cases, and access to digital records. Notably, it has a case management system that automates the assignment of cases to judges, uses inputs from the e-filing system to create a case record.[81] This system randomly assigns cases to judges. The system builds on an earlier system for clearance of backlog to enforce strict case flow management rules[82] through tracking and monitoring the performance of judges and courts. It also has a feature whereby lawyers can electronically inform the court that they have reached the court premises, following which the Queue Management System (QMS) will assign them a place in the queue of cases to be heard on that date.

Digitisation was implemented separately for the civil courts and for sharia courts, which are independent from each other. The e-Sharia system is therefore independent from the E-Courts system used by the civil courts.[83]

AUTHORITY

The E-Courts division of the office of the Chief Registrar of the Federal Court of Malaysia is responsible for overseeing the implementation of the E-Courts system. [84] The ultimate responsibility for the implementation is with the judiciary, largely free from the control of other branches of government, apart from matters of budgeting. The design of the system and the technological development for it, however, were outsourced to a private sector company.[85] E-Sharia, however, is overseen by the Shariah Judiciary Department of Malaysia.[86]

LEGAL FRAMEWORK

Malaysia did not implement a legal framework for digitisation.[87] This has led to a few problems as the implementing authority has no clearly defined mandate or obligations. There is no accountability framework for the management of the information system, leading to loss of or tampering with records.

PROCEDURAL LAW

Procedural law was amended in specific instances to allow digitisation to be implemented, where required. For example, the Criminal Procedure Code[88] of Malaysia required that evidence be recorded in the magistrates' own handwriting, which prevented the implementation of information management systems to the criminal courts, until subsequent legislation modified this requirement.[89]

---

[81] Arifin Zakaria. 2013. 'Review of ICT Implementation Mechanism in Judiciary of Malaysia.' Paper presented at the 'International Seminar on ITC Implementation in Courts.' Bukhara, Uzbekistan, September 18. Cited in Heike Gramckow et al. 2013. 'Good practices for Courts: Helpful Elements for Good Court Performance and the World Bank's Quality of Judicial Process Indicators'. *World Bank*. Available at http://documents.worldbank.org/curated/en/465991473859097902/pdf/108234-WP- GoodPracticesforCourtsReport-PUBLIC-ABSTRACT-EMAILED.pdf (accessed on 18 July 2019).

[82] The rules have timelines for case disposal and they limit the reasons for adjournments.

[83] Wan Satirah Wan Mohd Saman and Abrar Haider.2012. 'Electronic Court Records Management: A Case Study'. *Journal of e-Government Studies and Best Practices*, 2012. Available at https://www.researchgate.net/profile/Wan_Satirah_Wan_Mohd_Saman/publication/290042096_Electronic_court _records_management_in_Malaysia_A_case_study/links/57c8055b08aec24de0440c05/Electronic-court-records- management-in-Malaysia-A-case-study.pdf (accessed on 18 July 2019).

[84] Chief Registrar, Federal Court of Malaysia. 2019. *'The Chief Registrar Federal Court Of Malaysia'*. 25 July 2019. Available at http://www.kehakiman.gov.my/en/about-us/chief-registrars-office/division- pkpmp/e-court-division (accessed on 18 July 2019).

[85] Saman and Haider. 'Electronic court records management: a case study.'

[86] Mohd Saman, Wan Satirah Wan and Haider, Abrar. 2012. 'Courtroom technology: a case study of Shariah court in Malaysia'. CONF-IRM 2012 Proceedings, 73.

[87] Zain, Nurul Aiqa Mohamad, Wan Satirah Wan Mohamad Saman, Saiful Farik Mat Yatin, Abdul Rahman, Norshila Saifuddin Ahmad, Wan Nor Haliza Wan Mokhtar, and Nik Nurul Emyliana Nik Ramlee. 'Developing Legal Framework for E-Court in Judicial De-livery.' *International Journal of Engineering & Technology* 7, no. 3.7 (2018): 202-205.

[88] Section 266, Criminal Procedure Code (1999), Act 593.

[89] As per Saman and Haider. 'Electronic court records management', 'Act (Act 1350(2009) section 272C & 272D under Chapter 25 was amended to the effect that gave permission to allow court proceeding by mechanical means'.

IMPLEMENTATION STRATEGY

The judiciary engaged users in the design of the system, and conducted pilot projects in 11 courts to test them. Further, court user surveys were conducted to gauge the satisfaction of court users with new processes such as e-filing. In addition, help desks and other support was made available.[90]

DATA DISCLOSURE

There is no federal right to information in Malaysia. Two states, Penang and Selangor, have passed right to information legislations, but they only apply to departments of the governments of those states. There is no statutory provision for a citizen to request information about any information not published voluntarily by the judiciary.

The judiciary does proactively publish monthly statistics on the volume of cases filed, pending, and disposed,[91] but those are only available at the national level. Detailed data and statistics on the performance of the judiciary are provided in the annual reports of the judiciary.[92]

> ***"The E-Courts portal does not contain any claims of compliance with any accessibility standard, as per the authors' own observations. Some accessibility features are available, such as the ability to change text size, colour, and contrast."***

[90] Heike P. Gramckow, Erica Bosio, Silva Mendez and Jorge Luis. 2013. 'Good practices for Courts: Helpful Elements for Good Court Performance and the World Bank's Quality of Judicial Process Indicators'.

[91] Chief Registrar, Federal Court of Malaysia. 2019 'Statistics'. *Chief Registrar, Federal Court of Malaysia*. Available at http://www.kehakiman.gov.my/en/statistics (accessed on 20 July 2019).

[92] Chief Registrar, Federal Court of Malaysia. 2019. 'Annual Report of Judiciary'. *Chief Registrar, Federal Court of Malaysia*. Available at http://www.kehakiman.gov.my/en/annual-report-judiciary (accessed on 20 July 2019).

A notable recent development is the creation of an online repository of court judgements,[93] which is in beta testing at the time of writing (July 2019).

ACCESSIBILITY

The E-Courts portal[94] does not contain any claims of compliance with any accessibility standard, as per the authors' own observations. Some accessibility features are available, such as the ability to change text size, colour, and contrast. A test using the online test tools WAVE[95] did show some minor issues such as the lack of alternate text for some images and icons, but it does have some accessibility features. The lack of adoption of specific standards is a broader issue with the Malaysian E-Courts system, one which has also affected accessibility.

MANAGING TRANSITIONS

Stakeholder-specific guidance is available,[96] as are phone helplines, for the use of the E-Courts services. However, user guidance was insufficient to help users adapt in the early stages.[97] While there was a marked improvement in the efficiency of courts, maintenance of records suffered due to the lack of guidelines and regulations for record keeping.[98]

[93] Malaysian Judgments is a joint initiative of the Malaysian Judiciary, Asean Legal Information Centre (Asean LIC) and Malaysian Law Deans Council. 2018. 'Judgements. Malaysian Judgements. Available at http://www.judgments.my (accessed on 20 July 2019).

[94] Chief Registrar, Federal Court of Malaysia. 2019. 'E-courts Portal'. *Chief Registrar, Federal Court of Malaysia*. Available at https://ecourt.kehakiman.gov.my/ (accessed on 20 July 2019).

[95] WAVE. 2001. *WAVE*. Available at http://wave.webaim.org/ (accessed on 20 July 2019).

[96] For example, see "Omesti. 'eCourts Malaysia Phase 2 Law Firm Training - Release 1'. *Office of the Chief Registrar, Federal Court of Malaysia*. Available at http://www.kehakiman.gov.my/sites/default/files/ManualLatihanBhgn1.pdf (accessed on 20 July 2019).

[97] Zain et al. 'Developing Legal Framework for E-Court in Judicial De-livery.'

[98] Saman and Haider 'Electronic court records management: a case study.'

OVERVIEW

	ACCOUNTABILITY 	OPEN DATA 	ACCESSIBILITY 
United Kingdom	HMCTS is an agency of the Ministry of Justice. It is subject to joint oversight by the Lord Chief Justice and Lord Chancellor, and must respond to Parliamentary questions.	Aggregate statistics are published online. The Freedom of Information Act, 2000 exempts court records, but does compel HMCTS to publish details of its releases.	HMCTS websites are screen reader compatible and are compliant with Web Content Accessibility Guidelines (WCAG) 1.0 level AA.
Australia	Federal courts are administered by one authority, which has an equivalent in each state. There is a digital transformation agency for public services under the Prime Minister's cabinet that the federal courts are aligned with.	Court records are exempt under the Freedom of Information Act. Court authorities at the federal and state level publish statistics about judicial performance.	Federal court websites are designed to comply with the Web Content Accessibility Guidelines version 2.0.[1] Websites can be accessed through assistive technology for differently-abled people and PDF versions of judgments are available.
Canada	Courts are administered by their respective federal/provincial ministry of justice, typically through Court Services Branches. Court services only have access to case-related information, with judicial information being maintained out of their reach.	There is no explicit legislative policy on open data. The government releases action plans every 2 years to govern open data norms. Federal and provincial courts publish reports annually or bi-annually.	Canadian courts publish information in English and French. The provinces publish varying levels of case information. The Supreme Court website provides user friendly and simplified information.
Malaysia	Except for budgeting, the judiciary has control of the e-courts system through the Chief Registrar of the federal court. However, there is no legal framework for digitisation and the implementation of the system was outsourced to a private sector company.	There is no federal right to information, and state acts exempt the judiciary. Statistics on judicial performance are only available at the national level through annual reports.	There are no claims of compliance with any accessibility standard. Some accessibility features such as changes in text size, colour and contrast are available, but in a limited manner.

[1]Federal Courts Australia. 'Accessibility'. Available at https://www.fedcourt.gov.au/accessibility; (accessed on 16 July 2019).
Southern Australia Courts. 'Accessibility' Available at http://www.courts.sa.gov.au/Information/Pages/site-accessibility.aspx (accessed on 16 July 2019).

Conclusion

This paper discusses one of the key requirements of realising the vision of a Next Generation Justice Platform, and to provide a means of regulating the platform's design and operation, thereby ensuring that it always meets the needs of citizens. Regulating the platform through legislation is one way to ensure that the operation of the justice platform is democratic and responsive to citizens. It gives statutory backing to the conduct of judicial tasks on the platform, as well as to the platform authority. It also provides a means for the redressal of grievances and violations of rights, ranging from individual cases of misuse or technical malfunctions to accountability at various levels.

It is necessary to learn from the valuable experiences gained from the implementation of E-Courts so far, and to take steps towards the next stage in the evolution of the judiciary as a digital institution. The necessity of a legal framework is one of these insights, as legal recognition of electronic processes, which has been done at a broad level for other branches of government with the IT Act, is necessary to ensure that online judicial services can be held to the prescribed standards.

Like the previous two papers in this series, it serves as a starting point for a discussion regarding the future of the judiciary, and how it may operate through a digital platform. There are numerous questions that emerge from these ideas, ranging from the appropriate composition and oversight of the platform authority to the role of lawyers and administrative staff in a system where many tasks can be automated. The applicability of future data laws to the judiciary, and the question of whether it needs its own data laws given how frequently it needs to use sensitive information, is another question that can only be resolved through discussion.

The next stage of making this vision a reality is to begin this discussion, and to communicate with appropriate stakeholders regarding each question. The judiciary and implementing agencies would ideally maintain engagement with future users in each role, whether lawyers, citizens or judges, in order to ensure that the platform and the eventual platform authority responsible for its design are responsive to their needs. External experts in relevant areas would also need to be engaged with for their inputs.

Appendix I: Draft Personal Data Protection Bill

A host of comprehensive regulatory frameworks have been implemented globally to protect individuals' rights when their information is processed. Recognising a need for a similar framework in India, the Ministry of Electronics and Information Technology constituted a committee of experts under the Chairmanship of Justice (retd.) B. N. Srikrishna in July 2017, shortly before the *Puttaswamy* judgment was delivered.[99] The task of the committee was to examine the issues pertaining to data protection in India in order to both recommend methods to address them and to draft a data protection Bill. The draft Bill was presented to the Ministry of Electronics and Information Technology on 27 July 2018. On 11 December 2019 Ravi Shankar Prasad, the Minister of Electronics and Information Technology, introduced the Personal Data Protection Bill, 2019, with significant changes from the draft Bill. The Bill was referred to a Standing Committee headed by Shashi Tharoor, a Member of Parliament Lok Sabha, which is, at the time of the publication of this Paper, expected to submit their report by the end of the Budget Session of Parliament, 2020.

The Personal Data Protection Bill, 2019 aims to secure the autonomy and privacy of individuals by protecting their data. It establishes a regulatory body called the Data Protection Authority that will oversee data processing activities, provide for standards and rules regarding how data may be processed, and register independent data auditors to oversee compliance. The Bill creates legal obligations for anyone collecting or processing data and grants data rights to individuals such as the rights to data portability, data erasure and to access data on yourself, among others. The Bill defines two types of protected data: personal data and sensitive personal data. Personal data is any information about the characteristics or attributes of an individual, and includes any data inferred from personal data. Sensitive personal data is a list of especially private information like sexual orientation, caste, and biometric, financial and health data. Anonymised data is excluded from the purview of the Bill, though the Central Government is empowered to create policies on it as well as demand it from data processors and fiduciaries.

There are different grounds on which these two types of data may be processed. The State may process personal data without consent[100]:

1. **If it is necessary for the following functions of the State, as authorized by law:**

   a. The provision of any service or benefit.
   b. The issuance of any certificate, license or permit to the individual.

2. **If it is authorised by a law passed by Parliament or a state legislature.**

3. **For compliance with an order by a court or tribunal.**

4. **To respond to a medical emergency of individuals or public health crises like epidemics.**

5. **To provide safety measures during disasters or breakdowns of public order.**

The Bill also has an entire chapter that carves out several exemptions from the provisions of the Bill, largely for the State. The Central Government may exempt the processing of personal data by any agency of the government from any or all provisions of the Bill, subject to rules that it may prescribe. This exemption must come through an order and can only be issued if the Central Government is satisfied that it is necessary or expedient:[101]

1. **In the interest of sovereignty and integrity of India, the security of the state, friendly relations with foreign states, public order; or**

[99] Justice K S. Puttaswamy (Retd) vs Union of India (2017) 10 SCC 1, 24-08-2017.

[100] Section 12, Personal Data Protection Bill, 2019.

[101] Section 35, Personal Data Protection Bill, 2019.

2. **For preventing incitement to the commission of any cognizable offence relating to the reasons mentioned above.**

Section 36 also removes the applicability of a majority of the data protection provisions like data rights and the grounds for processing personal or sensitive personal data so long as the data processing is 'fair and reasonable' and adequate security measures are in place.[102] Some of the scenarios mentioned are pertinent to the justice system such as:

1. **Where personal data is processed for the prevention, detection, investigation and prosecution of any offence or contravention of law.[103]**

2. **Where disclosure of personal data is necessary for enforcing any legal right or claim, seeking any relief, defending any charge, opposing any claim, or obtaining any legal advice from an advocate in any impeding legal proceeding.[104] or**

3. **Where processing of personal data by any court or tribunal in India is necessary for the exercise of any judicial function.[105]**

There are two broad categories for the usage of personal data in the justice system – mere disclosure and the more extensive category, processing. Section 40 of the Bill also empowers the Authority to create a temporary regulatory environment with modified provisions[106] in order to foster innovations in artificial intelligence, machine learning or any other emerging technology in public interest.

[102] Section 36, Personal Data Protection Bill, 2019.

[103] Section 36(a), Personal Data Protection Bill, 2019.

[104] Section 36(b), Personal Data Protection Bill, 2019.

[105] Section 36(c), Personal Data Protection Bill, 2019.

[106] Referred to as a 'sandbox'.

References

1. Andhra Pradesh Civil Rules of Practice, 1990
2. Article 227, Clause 2, Constitution of India, 1950.
3. Section 6, Information Technology Act, 2000.
4. Section 12, Personal Data Protection Bill, 2019
5. Section 35, Personal Data Protection Bill, 2019
6. Section 36, Personal Data Protection Bill, 2019
7. Section 36(a) Personal Data Protection Bill, 2019
8. Section 36(b) Personal Data Protection Bill, 2019
9. Section 36(c) Personal Data Protection Bill, 2019
10. Section 52(d), Indian Copyright Act, 1957.
11. Section 266, Criminal Procedure Code (1999) Act 593. (Malaysia)
12. Recital (20), GDPR, 2016 Available at http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf (accessed on 5 September 2019).
13. GDPR Recitals and Articles. Availble at https://ico.org.uk/media/about-the-ico/disclosure-log/2014536/irq0680151-disclosure.pdf (accessed on 5 September 2019).
14. Criminal Practice Directions – October 2015 as amended April 2015 & November 2016 (UK). Available at https://webarchive.nationalarchives.gov.uk/20171010144459/http://www.justice.gov.uk/courts/procedure-rules/criminal/practice-direction/2015/crim-practice-directions-II-preliminary-proceedings-2015.pdf (accessed on 16 July 2019).
15. Courts Administration Legislation Amendment Act 2016 (Australia). Available at https://www.legislation.gov.au/Details/C2016A00024 (accessed on 16 July 2019).
16. Justice K S. Puttaswamy (Retd) vs Union of India (2017) 10 SCC 1, 24-08-2017.
17. Naresh Shridhar Mirajkar vs. State of Maharashtra, 1966 SCR (3) 744.
18. Swapnil Tripathi vs. Supreme Court of India, WRIT PETITION (CIVIL) NO. 1232 OF 2017.
19. Sri Vasunathan vs The Registrar General. W.P. No. 62038 (2016). Available at http://judgmenthck.kar.nic.in/judgmentsdsp/bitstream/123456789/224604/1/WP62038-16-23-01-2017.pdf (accessed on 5 September 2019)
20. Gary P. Johnston and David V. Bowen. 2005. 'The benefits of electronic records management systems: a general review of published and some unpublished cases'. *Records Management Journal*, 15(3), pp.131-140.
21. Shampa Paul. 2007. 'A case study of E-governance initiatives in India'. *The International Information & Library Review*, 39(3-4), pp.176-184.
22. Marco Velicogna. 2007. 'Justice systems and ICT what can be learned from Europe?' *Utrecht Law Review*, 3(1): 129 -147.
23. Anupam Chander. 2016. 'The racist algorithm' *Michigan Law Review*, 115, p.1023. Available at. https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1657&context=mlr (accessed on 5 September 2019).
24. Assisted digital and digital take-up community. 2016. 'Designing assisted digital support'. *gov.uk*. Updated July 2018. Available at https://www.gov.uk/service-manual/helping-people-to-use-your-service/designing-assisted-digital (accessed on 16 July 2019).
25. Australian Government, Digital Transformation agency. 'About us'. *Australian Government, Digital Transformation agency*. Available at https://www.dta.gov.au/about-us (accessed on 16 July 2019).
26. Australian Government. 'About'. *Australian Government*. Available at https://data.gov.au/ (accessed on 16 July 2019).
27. Barbara Ubaldi. 2013. 'Open Government Data: Towards Empirical Analysis of Open Government Data Initiatives', OECD Working Papers on Public Governance No. 22. OECD. Available at https://www.oecd ilibrary.org/docserver/5k46bj4f03s7en pdf?expires=1566549947&id=id&accname=guest&check-sum=EA96149567C690BD8D3BAACB4F2A0AF0 (accessed on 23 August 2019).
28. Bo Cowgill and Catherine Tucker. 2017. 'Algorithmic bias: A counterfactual perspective'. *NSF Trustworthy Algorithms*. Available at http://trustworthy-algorithms.org/whitepapers/Bo%20Cowgill.pdf (accessed on 5 September 2019).
29. Cabinet Office (UK). 2015. 'Open Standards principles' Updated April 2018. *Cabinet Office (UK)*. Available at https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles (accessed on 16 July 2019).
30. Centre for Budgeting, Governance, and Accountability (CBGA) and DAKSH. 2018. 'Memorandum to the Fifteenth Finance Commission on Budgeting for the Judiciary in India. CBGA and DAKSH. Available at http://dakshindia.org/wp-content/uploads/2019/06/Memorandum-on-Budgeting-for-Judiciary-in-India-from-CBGA-Website.pdf (accessed on 5 September 2019).
31. Committee of Experts under the Chairmanship of Justice B.N. Srikrishna. 2018. 'A Free and Fair Digital Economy Protecting Privacy, Empowering Indians'. *Ministry of Electronics and Information Technology, Government of India.*
32. Court Administrations Service Authority. 'Role and Mandate'. *Court Administrations Service Authority*. Available at http://www.cas-satj.gc.ca/en/about/mandate.shtml; (accessed on 16 July 2019).
33. Court Administrative Authority of Southern Australia. 'Strategic plan'. *Southern Australia Courts*. Available at http://www.courts.sa.gov.au/OurCourts/CourtsAdministrationAuthority/Pages/default.aspx (accessed on 16 July 2019).
34. Courts and Tribunals Judiciary (UK). 'Accessibility'. *Courts and Tribunals Judiciary (UK)*. Available at https://www.judiciary.uk/accessibility/ (accessed on 16 July 2019).
35. Courts and Tribunals Judiciary. 'Judgements'. *Courts and Tribunals Judiciary (UK)*. Available at https://www.judiciary.uk/judgments/ (accessed on 16 July 2019).

36. E-Committee, Supreme Court of India. 2005. 'National Policy and Action Plan for Implementation of Information and Communication Technology in the Indian Judiciary'. *E-Courts*. Available at https://sci.gov.in/pdf/ecommittee/action-plan-ecourt.pdf. (accessed on 23 August 2019).

37. Federal Australian Courts. 'Corporate plan (2018-19)'. *Federal Australian Courts*. Available at https://www.fedcourt.gov.au/__data/assets/pdf_file/0007/51892/Corporate-Plan-2018-19.pdf (accessed on 16 July 2019).

38. Federal Court of Australia. 2015. Case study documenting a transition to electronic case files. Federal Court of Australia. Available at http://www.naa.gov.au/information-management/digital-transition-and-digital-continuity/digital-excellence-awards/federal-court-of-australia.aspx (accessed 16 July 2019)

39. Federal Courts Australia. 'Accessibility'. *Federal Courts Australia*. Available at https://www.fedcourt.gov.au/accessibility (accessed on 16July 2019).

40. Federal Courts Australia. 'Annual Reports'. *Federal Courts Australia*. Available at https://www.fedcourt.gov.au/digital-law-library/annual-reports (accessed on 16July 2019).

41. Flores, A.W., Bechtel, K. and Lowenkamp, C.T., 2016. 'False Positives, False Negatives, and False Analyses: A Rejoinder to "Machine Bias: There's Software Used across the Country to Predict Future Criminals. And It's Biased against Blacks."' *Federal Probation*, 80, p.38. Available at https://www.researchgate.net/profile/Christopher_Lowenkamp/publication/306032039_False_Positives_False_Negatives_and_False_Analyses_A_Rejoinder_to_Machine_Bias_There%27s_Software_Used_Across_the_Country_to_Predict_Future_Criminals_And_it%27s_Biased_Against_Blacks/links/57ab619908ae42ba52aedbab/False-Positives-False-Negatives-and-False-Analyses-A-Rejoinder-to-Machine-Bias-Theres-Software-Used-Across-the-Country-to-Predict-Future-Criminals-And-its-Biased-Against-Blacks.pdf

42. Geothink, 'Citizens guide to open data'. Open data and privacy. *Geothink*. Available at https://citizens-guide-open-data.github.io/ (accessed on 16 July 2019)

43. Giampiero Lupo and Jane Bailey. 2014. 'Designing and Implementing e-Justice Systems: Some Lessons Learned from EU and Canadian Examples', *Open Access Journal*, 3(2): 1-35.

44. Government of Canada,' Multi Stakeholder forum'. *Government of Canada.* Available at https://open.canada.ca/en/multi-stakeholder-forum-open-government (accessed on 16 July 2019).

45. Government of Canada. 'Open Data Principles'. *Government of Canada*. Available at *https://open.canada.ca/en/open-data-principles* (accessed on 16 July 2019).

46. Government of Canada. 2018 -2019. 'National Action plan'. *Government of Canada*. Available at https://open.canada.ca/en/content/canadas-2018-2020-national-action-plan-open-government#toc3-5. (accessed on 16 July 2019).

47. Heike Gramckow, Ebeid, Omniah Ebeid, Erica Bosio, Silva Mendez and Jorge Luis. 2016. 'Good Practices for Courts: Helpful Elements for Good Court Performance and the World Bank's Quality of Judicial Process Indicators.' World Bank. Available at http://documents.worldbank.org/curated/en/465991473859097902/pdf/108234-WP-GoodPracticesforCourtsReport-PUBLIC-ABSTRACT-EMAILED.pdf (accessed on 16 July 2019)

48. HMCTS. 2014. Framework Document. *HMCTS*. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/384922/hmcts-framework-document-2014.pdf (accessed on 16 July 2019)

49. HMCTS. 2018. 'HMCTS reform events programme'. *HMCTS*. Updated July 2019. Available at https://www.gov.uk/guidance/hmcts-reform-events-programme (accessed on 16 July 2019).

50. HMCTS. 2018. 'Engaging with our external stakeholders'. *HMCTS*. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759859/HMCTS060_ExternalStakeEngageApproach_FINAL.pdf (accessed on 17 July 2019).

51. HMCTS. 2019. 'HMCTS FOI Releases 2019'. *HMCTS* Available at https://www.gov.uk/government/publications/hmcts-foi-releases-2019 (accessed on 16 July 2019).

52. Jane Bailey. 2012. 'Digitization of Court processes in Canada', Cyber Justice laboratory, *Onatrio and BC study*. Available at https://www.cyberjustice.ca/files/sites/102/WP002_CanadaDigitizationOfCourtProcesses20121023.pdf. (accessed on 16 July 2019).

53. Ken Krechmer. 1998. 'The principles of open standards' Standards Engineering, 50(6), pp.1-6.

54. Law Society of England and Wales. 2019. 'Written evidence from The Law Society (CTS0040)' (regarding Court and Tribunals Reforms Inquiry). parliament.uk. Available at http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/justice-committee/hmcts- court-and-tribunal-reforms/written/97774.html (accessed on 17 July 2019).

55. Lord Chancellor, the Lord Chief Justice and the Senior President of Tribunals. 2016. 'Transforming Our Justice System'. *Ministry of Justice* (*UK*). Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/553261/joint-vision-statement.pdf (accessed on 16 July 2019).

56. Malaysian Judiciary, Asean Legal Information Centre (Asean LIC) and Malaysian Law Deans Council. 2018. 'Judgements.' Available at http://www.judgments.my (accessed on 20 July 2019).

57. Mike Brazier. 2018. 'Helping people to use online services'. Inside HMCTS. *HMCTS*. Available at https://insidehmcts.blog.gov.uk/2018/06/28/helping-people-to-use-online-services/ (accessed on 16 July 2019).

58. Ministry of Electronics and Information Technology, Government of India. 2018. 'National e-Governance Plan'. Ministry of Electronics and Information Technology, Government of India. Available at https://meity.gov.in/divisions/national-e-governance-plan (accessed on 23 August 2019).

59. Ministry of Justice (UK). 'Statistics at MOJ'. *Ministry of Justice* (*UK*). Available at https://www.gov.uk/government/organisations/ministry-of-justice/about/statistics (accessed on 16 July 2019).

60. Ministry of Justice (UK). 2014. 'Criminal justice system: data standards forum guidance'. *Ministry of Justice* (*UK*). Updated April 2019. Available at https://www.gov.uk/guidance/criminal-justice-system-data-standards-forum-guidance#cjs-standards-and-open-standards (accessed on 16 July 2019).

61. Ministry of Justice (UK). 2017. 'Notes on Practice Directions'. *Ministry of Justice* (*UK*). Updated January 2017. Available at https://www.justice.gov.uk/courts/procedure-rules/civil/rules/raprnotes (accessed on 16 July 2019).

62. Ministry of Science and Technology, Government of India, 2012. 'National Data Sharing and Accessibility Policy'. *Ministry of Science and Technology, Government of India*. Available at https://data.gov.in/sites/default/files/NDSAP.pdf (accessed on 23 August 2019).

63. Nurul Aiqa Mohamad Zain, Wan Satirah Wan Mohamad Saman, Saiful Farik Mat Yatin, Abdul Rahman, Norshila Saifuddin Ahmad, Wan Nor Haliza Wan Mokhtar, and Nik Nurul Emyliana Nik Ramlee. 'Developing Legal Framework for E-Court in Judicial De-livery.' *International Journal of Engineering & Technology* 7, no. 3.7 (2018): 202-205.

64. Nurul Aiqa Mohamad Zain. 2018. 'Developing Legal Framework for E-Court in Judicial Delivery'. *International Journal of Engineering & Technology*. 7 (3.7): 202-205.

65. OECD (2013), 'Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines', OECD Digital Economy Papers, No. 229. *OECD Publishing, Paris*. Available at http://dx.doi.org/10.1787/5k3xz5zmj2mx-en (accessed on 5 September 2019).

66. Office of the Chief Registrar, Federal Court of Malaysia. 2019. 'Statistics'. *Office of the Chief Registrar, Federal Court of Malaysia*. Available at http://www.kehakiman.gov.my/en/statistics (accessed on 20 July 2019).

67. Office of the Chief Registrar, Federal Court of Malaysia. 2019. 'Annual Report of Judiciary'. *Office of the Chief Registrar, Federal Court of Malaysia*. Available at http://www.kehakiman.gov.my/en/annual-report-judiciary (accessed on 20 July 2019).

68. Office of the Chief Registrar, Federal Court of Malaysia. 2019. 'E-courts Portal'. *Office of the Chief Registrar, Federal Court of Malaysia*. Available at https://ecourt.kehakiman.gov.my/ (accessed on 20 July 2019).

69. Office of the Chief Registrar, Federal Court of Malaysia. 2019. *Office of the Chief Registrar, Federal Court of Malaysia,* 25 July 2019. Available at http://www.kehakiman.gov.my/en/about-us/chief-registrars-office/division-pkpmp/e-court-division (accessed on 18 July 2019).

70. Ontario Court of Justice. 'Memorandum of understanding'. *Ontario Court of Justice*. Available at http://www.ontariocourts.ca/ocj/memorandum-of-understanding/. (accessed on 16 July 2019).

71. Ontario Court of Justice. 'Court Statistics'. *Ontario Court of Justice*. Available at http://www.ontariocourts.ca/ocj/statistics/ (accessed on 16 July 2019).

72. Provincial Court of British Columbia. 'Annual report 2017-2018'. *Provincial Court of British Columbia*. Available at https://www.provincialcourt.bc.ca/downloads/pdf/AnnualReport2017-2018.pdf (accessed on 16 July 2019).

73. Provincial Court of British Columbia. 'Court Reports'. *Provincial Court of British Columbia.* Available at https://www.provincialcourt.bc.ca/news-reports/courtreports (accessed on 16 July 2019).

74. Rahul Mathan. 2017. 'Beyond Consent: a New Paradigm for Data Protection'. *The Takshashila Institution*. Available at http://takshashila.org.in/wp-content/uploads/2017/07/TDD-Beyond-Consent-Data-Protection-RM-2017-03.pdf (accessed on 5 September 2019)

75. Rahul Matthan, Manasa Venkataraman, and Ajay Patri. 2018. 'A Data Protection Framework for India'. *The Takshashila Institution*. February 2018. Available at http://takshashila.org.in/wp-content/uploads/2018/02/TPA-Data-Protection-Framework-for-India-RM-MV-AP-2018-01.pdf (accessed on 5 September 2019)

76. Southern Australia Courts. 'Accessibility'. *Southern Australia Courts.* Available at http://www.courts.sa.gov.au/Information/Pages/siteaccessibility.aspx (accessed on 16 July 2019).

77. Southern Australia Courts. 'Court performance statistics'. *Southern Australia Courts.* Available at http://www.courts.sa.gov.au/OurCourts/CourtsAdministrationAuthority/statistics/Pages/Court-Performance-Statistics.aspx (accessed on 16 July 2019).

78. Supreme Court of Canada. 'Case information'. *Supreme Court of Canada.* Available at https://www.scc-csc.ca/case-dossier/cb/index- eng.aspx. (accessed on 16 July 2019).

79. Wan Satirah Wan Mohd Saman and Abrar Haider. 2012. 'Courtroom technology: a case study of Shariah court in Malaysia'. CONF-IRM 2012 Proceedings, 73.

80. Wan Satirah Wan Mohd Saman and Abrar Haider. 2012. 'Electronic court records management: a case study' (Doctoral dissertation, IBIMA-International Busines Information Management Association). Available at https://www.researchgate.net/profile/Wan_Satirah_Wan_Mohd_Saman/publication/290042096_Electronic_court _records_management_in_Malaysia_A_case_study/links/57c8055b08aec24de0440c05/Electronic-court-records- management-in-Malaysia-A-case-study.pdf (accessed on 18 July 2019).

81. WAVE. 2001. *WAVE*. Available at http://wave.webaim.org/ (accessed on 20 July 2019).

82. Legal Aid Agency. 2015. 'Crime news: national rollout for Crown Court Digital Case System'. *gov.uk*. Available at https://www.gov.uk/government/news/crime-news-national-rollout-for-crown-court-digital-case-system (accessed on 16 July 2019).

83. Financial Times. 2018. 'Court modernisation project risks missing 2023 deadline', *Financial Times*, May 8 2018. Available at https://www.ft.com/content/1e1542c2-4f93-11e8-9471-a083af05aea7

84. Owen Bowcott and Pamela Duncan. 2019. 'Half of magistrates courts in England and Wales closed since 2010. *The Guardian*. 27 January 2019. https://www.theguardian.com/law/2019/jan/27/half-of-magistrates-courts-in-england-and-wales-closed-since-tories-elected, and Law Society of England and Wales. 2019. 'Written evidence from The Law Society (CTS0040)'

85. Owen Bowcott. 2019. 'Law courts in chaos as IT meltdown disrupts thousands of cases'. *The Guardian*, 23 January 2019. Available at https://www.theguardian.com/law/2019/jan/23/law-courts-in-chaos-as-it-meltdown-disruptxs-thousands-of-cases (accessed on 17 July 2019).

86. National Post. 2015. Ontario admits it blew $4.5-million on failed court modernization project. *National Post*. Available at https://nationalpost.com/news/canada/ontario-admits-it-blew-4-5-million-on-failed-court-modernization-project. (accessed on 16 July 2019).

87. Kristen Robinson. 2019. 'B.C. Attorney General looking to use digital technology to improve access to justice', *Global News*, 3 June 2019. Available at https://globalnews.ca/news/5347134/bc-attorney-general-digital-court-update/. (accessed on 16 July 2019).

DAKSH

63 Palace Road
Vasanthnagar
Bengaluru 560052