VOLUME 8 FALL 2021 ISSUE I

NLUJ LAW REVIEW

8(1) NLUJ Law Review (2021)

A NATIONAL LAW UNIVERSITY JODHPUR PUBLICATION

VOLUME 8 **FALL 2021** **ISSUE 1**

NLUJ LAW REVIEW

VOLUME 8 **FALL 2021** **ISSUE 1**

NLUJ LAW REVIEW

LONG ARTICLES

SHORT ARTICLES

Vini Singh, *Striking the Right (to be forgotten) Balance: Reconciling Freedom of Speech and Privacy – Dignity – Autonomy*, 8(1) NLUJ L. REV. 1 (2021).

STRIKING THE RIGHT (TO BE FORGOTTEN) BALANCE: RECONCILING FREEDOM OF SPEECH AND PRIVACY – DIGNITY – AUTONOMY

*Vini Singh**

ABSTRACT

Technology has transformed the way we share and access information. One only needs to run a simple Google search to meet a person's online persona. The abundant and long-lasting digital memory undoubtedly has its advantages. At the same time, it has far-reaching implications for privacy-dignity-autonomy interests. While there may never have been a time throughout human history when people may have been fully in control of their persona, neither have they been so deprived of control over their public image. The right to be forgotten reflects the claim of an individual to control their persona by offering a chance to reinvent one's online persona by hiding and/or removing personal information from the internet. Since the internet is a primary medium of communication and a valuable source of information, the right to be forgotten poses a significant challenge to the effective exercise of free speech rights. For this reason, it has been the subject of debate across various jurisdictions, including India. The Personal Data Protection Bill, 2019, which is currently being

* The author is an Assistant Professor, Faculty of Law at National Law University, Jodhpur and may be contacted at **vini.hnlu@gmail.com**.

scrutinized by a Joint Parliamentary Committee seeks to introduce the right to be forgotten along with a right to correction and erasure of personal information. While the proposed legislation would mean a step forward in data protection, it fails to strike the appropriate balance between the competing free speech and privacy-dignity-autonomy rights in the context of the proposed right. The author analyses how these competing rights may be reconciled and how the right to be forgotten may be squared with free speech in India.

TABLE OF CONTENTS

I. INTRODUCTION

With the advancement in technology, our lives are becoming less and less private. The electronic devices we use, such as smartphones, fitness trackers, GPS monitors, smart speakers and televisions, constantly keep track of and upload our activities. Technology is so intrusive that to offer a personalised experience, every single search on the internet, every website visited, every video watched online, every song listened to or every post liked or shared by an individual, is compiled to create an online profile for them. This profile can then be used to predict and even manipulate their preferences, ranging from which mobile phone to buy to their political choices.[1]

Further, it is very easy for others to meet this online version of an individual. In fact, it often happens that people meet one's online version and rely on it before meeting them in person – both, in a personal and professional setting. It is not at all uncommon for admission committees or potential recruiters to conduct a google search on the applicants. Thus, making it possible for a single photograph or a social media post depriving a person of an educational or professional opportunity.[2] In extreme cases,

[1] Jane Wakefield, *Your data and how it is used to gain your vote*, BBC NEWS (June 11, 2021), https://www.bbc.com/news/technology-54915779.
[2] Dan Levin, *Colleges Rescinding Admissions Offers as Racist Social Media Posts Emerge*, THE NEW YORK TIMES (June 2, 2021), https://www.nytimes.com/2020/07/02/us/racism-social-media-college-admissions.html.

like instances of revenge pornography, it may humiliate, cause immense mental anguish and even drive a person to suicide.[3]

Howsoever reclusive a person might be, they cannot help having an online persona. They may delete their social media accounts out of personal preference, but they would still be required to maintain an online presence to access basic government facilities. For example, to get vaccinated against COVID-19 in India, individuals had to register themselves on the CoWIN web portal.[4] Similarly, payments that they make through credit/debit cards would still be collected and processed. Opting out of internet usage is hardly an option. It is so intertwined with our lives that access to internet services has been recognised as a fundamental right.[5] Moreover, opting out or being cautious on the internet would impede the exercise of their rights to speech and expression, information as well as education. Therefore, it is important that an individual should have control over the personal information that is collected, processed and shared with others.

The Court of Justice of the European Union [*hereinafter* "**CJEU**"] addressed these concerns by recognising the "*right to deindex personal information*" in *Google Spain SL v. Agencia Española de Protección de Datos*

---

[3] Kristen Zaleski, *The long trauma of revenge porn*, OUPBLOG (June 11, 2021), https://blog.oup.com/2019/09/the-long-trauma-of-revenge-porn/.

[4] Shruti Dhapola, *India's COVID 19 vaccine rollout strategy has a digital gap; here are those struggling to plug it*, THE INDIAN EXPRESS (June 11, 2021), https://indianexpress.com/article/technology/tech-news-technology/india-covid-19-cowin-portal-vaccine-rollout-strategy-has-a-digital-gap-those-trying-to-fix-it-7338250/.

[5] Anuradha Bhasin v. Union of India, 2020 SCC OnLine SC 1725; The Constitution of Greece 1975, art. 5A (1); *see also,* Cengiz and Others v. Turkey, [2015] ECHR 1052.

[*hereinafter* "***Google Spain***"].[6] The matter arose in Spain in 2010 when Mr. Mario Costeja Gonzalez brought a complaint before the Spanish Data Protection Agency. He sought the removal of a news item from 1998 regarding his bankruptcy posted on the website of the Spanish newspaper 'La Vanguardia'. The news item was indexed by Google and consequently displayed whenever a Google search for his name was done. He requested the newspaper to take down the news item as it was damaging to his reputation, particularly now that his bankruptcy was old news. When the newspaper refused, he approached Google to deindex the item from search results. Google's refusal to remove the results ensued the legal action. The National High Court of Spain referred the matter to the CJEU seeking a preliminary ruling on the obligation of internet search engines to remove or erase information published by third party websites. The CJEU declared that people have a right to request the removal of information regarding themselves if the said information was "*inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine*."

The CJEU observed that search engines often collect personal information. They index, store, and share such information with other users and "*play a decisive role in the overall dissemination of personal data.*"[7] The CJEU primarily relied on Article 12(b) of the European Union's Data Protection Directive [*hereinafter* "**DPD**"], which confers the right to seek rectification,

[6] Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12, ECLI: EU: C: 2014: 317.
[7] *Id.* at 34 – 36.

erasure or blocking of data the processing of which does not comply with the DPD. It also relied on Article 14(a) of the DPD that confers the right to object to processing of data on any of the legitimate grounds specified in the DPD. Further, it referred to Article 6(d) of the DPD that obligates the member states to ensure the relevance, accuracy and currency of personal data. Notably, the CJEU emphasised upon the need for balancing the right to privacy with freedom of expression and access to information. It observed that while considering a request to deindex, the right of the other individuals to access the information in question, the interest of the public in the information depending on the data subject's role in public life, the sensitivity of the information and its impact on data subject's life, and the data subject's right to privacy must be taken into account.[8]

Thereafter, the General Data Protection Regulation [*hereinafter* "**GDPR**"] was implemented in 2018, replacing the DPD. Article 17 of the GDPR guarantees the "*right to erasure (right to be forgotten)*". Subject to certain exceptions and the protection of other rights and interests such as freedom of expression, the right allows the data subjects to request for deletion of personal information held by data controllers "*without undue delay*". There is an obvious tension between the right to be forgotten and freedom of expression and access to information.

The internet is the new marketplace of ideas. Restricting access to information or removing it from the internet could prevent free trade of

[8] *Id.* at 81.

ideas and seems sacrilegious. People worry that an overbroad right in the hands of those wielding public power may distort democratic discourse.[9] It may create a culture of secrecy and be abused to silence the critics of the government, public agencies, and even those wielding huge private power. It may also have a significant chilling effect on freedom of speech and expression.

However, information on the internet is not as permanent as we believe it to be.[10] Search engine results are a product of algorithms and are ranked based on their relevance to the user. They are therefore subject to change. For instance, if user A runs a Google search on "the right to be forgotten" on a given date and time, it is not necessary that they will receive the same search results later. Some results that were displayed prominently before may be de-ranked, while other results may become more prominent. Similarly, OTT platforms, such as Netflix, acquire streaming rights from content providers for TV shows and movies. The content is only available to stream for the period of the license and is removed thereafter.

Further, content is frequently removed from the internet due to various reasons. For example, social media websites like Facebook and Twitter prescribe community standards. Violation of these community standards can lead to the removal of social media posts and in some cases, even blocking of the user's access to their account. Similarly, a notice of

---

[9] KRISTIE BYRUM, THE EUROPEAN RIGHT TO BE FORGOTTEN: THE FIRST AMENDMENT ENEMY (Rowman & Littlefield 2018).

[10] Meg Leta Ambrose, *It's About Time: Privacy, Information life Cycles, and the Right to be Forgotten*, 16 STAN. TECH. L. REV. 369, 372 -373(2013).

alleged copyright violation may lead to the immediate takedown of content.[11]

Therefore, a narrowly tailored right to be forgotten is not likely to bring a drastic change. It is only the remedy of erasure which involves the destruction or removal of personal data and allows takedown of content from the source website.[12] Further, the data that is subject to erasure may still be kept if it is anonymised.[13] Other remedies simply limit the accessibility of information. For instance, delisting/deindexing involves removal of links to the information from search results.[14] The content remains available on the source website. Likewise, de-ranking only makes a search result less prominent.[15] Further, flagging just marks a search result as unreliable or incorrect as the case may be,[16] and the remedies of rectification/correction and updating allow data subjects to correct incorrect personal data[17] and update outdated data, respectively.[18]

---

[11] Lyle Denniston, *Are copyright claims stifling free speech on the Internet?*, CONSTITUTION DAILY (June 11, 2021), https://constitutioncenter.org/amp/blog/are-copyright-claims-stifling-free-speech-on-the-internet.

[12] European Commission, *Do we always have to delete personal data if a person asks* (Oct. 8, 2021), https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/do-we-always-have-delete-personal-data-if-person-asks#:~:text=Data%20do%20not%20have%20to%20be%20deleted&text=The%20politician%20requests%20to%20remove,personal%20data%20is%20being%20processed.

[13] *Id.*

[14] CNIL, *The Right to de-listing in questions* (Oct. 8, 2021), https://www.cnil.fr/en/right-de-listing-questions.

[15] Edward Lee, *The Right to be Forgotten v. Free Speech*, 12 I/S: A JOURNAL OF LAW AND POLICY 85, 105(2015).

[16] Hannah Cook, *Flagging the Middle Ground of the Right to be Forgotten: Combating Old News with Search Engine Flags*, VAND. J. ENT. & TECH. L. 1(2020).

[17] The European General Data Protection Regulation 2016/679, art. 16.

[18] *Id.*

Since different jurisdictions reconcile competing rights differently, it is not possible to adopt the right to be forgotten guaranteed under the GDPR universally. Most jurisdictions rely on the context-based proportionality principle to balance competing rights which requires them to minimally impair each right only to the extent it is necessary and proportionate to protect the other rights in each context.[19] However, different jurisdictions ascribe different values to the rights in conflict. For instance, dignity is the most important value in Europe;[20] while Canada lays emphasis on multiculturalism, equality and dignity.[21] While interpreting and balancing fundamental rights this preference takes the spotlight and determines the result.

On the other hand, the USA does not apply the proportionality standard when freedom of speech is pitted against other rights. The First Amendment, which prohibits the US Congress from making a law abridging free speech, always trumps other rights.[22] Therefore, an Indian right to be forgotten would have to be squared with the Constitution of India [*hereinafter* "**the Constitution**"].[23] It would have to be designed in such a way that it effectively safeguards the privacy-dignity-autonomy rights

---

[19] ALEC STONE SWEET AND JUD MATHEWS, PROPORTIONALITY, BALANCING & CONSTITUTIONAL GOVERNANCE: A COMPARATIVE & GLOBAL APPROACH (Oxford University Press 2019); Robert Alexy, *Constitutional Rights, Balancing and Rationality*, 16(2) RATIO JURIS 131(2003).

[20] James Q. Whitman, *The Two Western Cultures of Privacy: Dignity versus Liberty*, 113 YALE LAW JOURNAL 1151(2004).

[21] Peter W. Hogg, *Interpreting the Charter of Rights: Generosity and Justification*, 20 OSGOODE HALL LAW JOURNAL 817(1990).

[22] FLOYD ABRAMS, THE SOUL OF THE FIRST AMENDMENT (Yale University Press 2017).

[23] INDIAN CONST. art. 13(2).

of individuals, and at the same time does not unreasonably encroach upon freedom of speech, expression and information.

While the debate surrounding the right to be forgotten has been focused on whitewashing one's embarrassing past, it is not only about remembering and forgetting, and the harms of extensive digital memory. The right to be forgotten is a corollary of informational autonomy or informational self-determination and represents the control an individual should be able to exercise over their personal data.

Part II of this paper highlights this aspect of the right to be forgotten. Part III traces the right across various jurisdictions. Thereafter, Part IV discusses the proposed design for the right to be forgotten in India. Next, Part V examines whether this proposed framework strikes the appropriate balance between freedom of speech and expression and privacy-dignity-autonomy rights in the context of the right to be forgotten. Finally, Part V also offers suggestions on how the right must be tailored to ensure its constitutional compatibility.

II. DEFINING THE RIGHT TO BE FORGOTTEN

The "right to be forgotten" emerged as a response to the threat posed by technology to privacy, reputation, identity, and memory. It allows for the reinvention of one's online persona by providing the means to hide and/or remove personal information from the internet.

The concept has been controversial since its introduction. It has elicited strong responses from across the world. Some have called it

"censorship"[24] while others have termed it as "rewriting history".[25] Those who argue for this right have also used different terms to describe it. The GDPR also uses the terms "right to erasure" and "right to be forgotten" alternatively. Likewise, the Indian Personal Data Protection Act, 2019 refers to the right as the "right to erasure" and the "right to correction". Viktor Mayer–Schönberger,[26] who is a key proponent of this right and Paul Bernal[27] refer to the right as a "right to delete"; while others call it the "right to oblivion" or "*droit à l'oubli*".[28]

These terms have different connotations and safeguard different interests. For instance, the terms "right to erasure" and "right to be forgotten" used in the GDPR refer to distinct concepts. The former enables a data subject to restrict the unlawful use of their personal data, while the latter allows the data subject to control the usage of their personal data through means like withdrawal of consent.[29] The purpose of the right to be forgotten is to ensure that data subjects have effective control of what they

---

[24] Robert G. Larson III, *Forgetting the First Amendment: How Obscurity Based Privacy and a Right to be Forgotten are Incompatible with Free Speech*, 18. COMM. L. & POL'Y 91, 108(2013)

[25] Antoon De Baets*, A Historian's View on the Right to be Forgotten*, 30 INT'L REV. L. COMP. & TECH. 57(2016).

[26] VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN A DIGITAL AGE (Princeton University Press 2009).

[27] Paul Bernal, *A Right to Delete?*, EJLT 1(2011).

[28] Eloise Gratton and Jules Polonetsky, *Droit a L'Oubli: Canadian Perspective on the Global Right to be Forgotten Debate*, 15 COLO. TECH. LAW JOURNAL 337(2017).

[29] Cecile de Terwangne*, The Right to be Forgotten and Informational Autonomy in a Digital Environment* in Alessia Ghezzi et. al. (eds.) NORBERTO NUNO ET AL, THE ETHICS OF MEMORY IN A DIGITAL AGE 82 (Palgrave Macmillan 2014).

put up online and are able to correct, withdraw or delete it all.[30] Likewise, the "right to oblivion" is distinct from the "right to erasure" and the "right to be forgotten". The "right to oblivion" arises only from a need to protect privacy interests and aims to remedy the potential harms to the "dignity, personality, reputation and identity of an individual."[31] On the other hand, the impetus of the "right to erasure" and the "right to be forgotten" is much broader – they are concerned with the informational flow rather than remembrance and forgetting. They also empower data subjects as there is a power imbalance between data subjects and data controllers.[32] Further, the "right to oblivion" would only cover data that is no longer relevant, while the "right to erasure" and the "right to be forgotten" would encompass inadequate, irrelevant, and excessive personal information as well.[33]

The right to be forgotten thus represents the idea of control over one's personal data. It can be derived from autonomy, dignity, reputation, personality, and privacy rights of an individual.[34] It is broad enough to include the remedies of erasure, delisting/deindexing, de-ranking, flagging, correction and updating that would ensure data subject's control over their personal data.

---

[30] *Fundamental Rights and Citizenship introduced the right to be forgotten along with other data protection reforms in the EU*, VIVIANNE REDING, THE EUROPEAN COMMISSIONER FOR JUSTICE; Steven C. Bennett, *The "Right to be Forgotten": Reconciling E.U. and U.S. Perspectives*, 30 BERKELEY J. INT'L L. 161(2012) ("**Bennett**").

[31] Meg Leta Jones and Jef Ausloos, *The Right to be Forgotten Across the Pond*, 3 J. OF INFO. POL'Y. 1(2013) ("**Meg Leta Jones**"); Aurelia Damo and Damien George, *Oblivion, Erasure and Forgetting in the Digital Age*, 5(2) JIPITEC 71(2014)

[32] Andrea Slane, *Search Engines and the Right to be Forgotten: Squaring the Remedy with Canadian Values on Personal Information Flow*, 55 OSGOODE HALL L. REV. 349(2018).

[33] Meg Leta Jones, *supra* note. 31.

[34] Rolf H. Weber, *The Right to be Forgotten: More than a Pandora's Box?*, JIPITEC 2(2011).

III. TRACING THE RIGHT TO BE FORGOTTEN

While the right to be forgotten is fairly novel, the underlying concept of controlling one's public image is quite well established. The right to autonomy over one's persona has been protected in numerous cases. For example, in the 1867 *Dumas* case, a photographer who had copyright over compromising images of the famous author Alexandre Dumas was prevented from publishing them and was compelled to sell the rights to Dumas. The French court pointed out that privacy, like other aspects of honour, could not be traded off; Dumas had a right to withdraw his consent as he was the subject of those photographs.[35] Similarly, in the Canadian case of *Aubry v. Editions Vice Versa*,[36] the 'Editions' magazine had published the photograph of a teenage girl without her consent. The Canadian Supreme Court upheld her right to privacy, personality and image and granted her damages as there was no predominant public interest in publishing the photograph.

There are several legal predecessors to the right to be forgotten. Different aspects of the right particularly the "right to oblivion" were recognised in several jurisdictions. For example, "Habeas Data" is a writ and constitutional remedy available in many jurisdictions such as Brazil, Colombia, Paraguay, Peru, Argentina, and the Philippines.[37] The remedy can be sought by an individual to find out what information is held about

---

[35] John W. Dowdell, *An American Right to be Forgotten*, 52 TULSA L. REV. 311, 317-318(2017).
[36] Aubry v. Editions Vice Versa, [1998] 1 S.C.R. 591 (Can.).
[37] Sarah L. Lode, *"You have the Data"…The Writ of Habeas Data and Other Data Protection Rights: Is the United States Falling Behind?,* 94 INDIANA L. J. 41, 43 -46(2019).

them, and to seek rectification or destruction of the said personal information. Likewise, in Germany, the rights of human dignity and personality have been expanded to include a "right to informational self-determination".[38] This right allows individuals to determine when and to what extent their personal information is published. Similarly, the French banking sector had the notion of "*droit à l'oubli numerique*".[39] It provided for deletion of information from databases after a certain period of time.

Furthermore, most jurisdictions recognise informational privacy as an important limb of the right to privacy. For example, in the USA, the Constitutions of Alaska, California, Florida, Illinois, and Washington guarantee the right to informational privacy.[40] It has also been recognised in several decisions of the Supreme Court of the United States.[41] Article 8 of the Charter of Fundamental Rights of the European Union also guarantees the right to protection of personal data.[42] It is also regarded as an important limb of the right to privacy-dignity-autonomy in India.[43]

Additionally, almost every jurisdiction, even the USA has a history of legal forgiveness and recognises that rehabilitation of criminals is an

---

[38] Gerrit Hornung and Christoph Schnabel, *Data Protection in Germany I: The population census decision and the right to informational self – determination*, 25 COMP. L. & SEC. REV. 84(2009).
[39] Maryline Boizard, *The right to respect for private life: an effective tool in the right to be forgotten?*, Special Issue: Privacy, MONTESQUIEU L. REV. 20(2015).
[40] Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH L. J. 1085, 1129 – 1144(2002).
[41] Riley v. California, 573 U.S. 373 (2014); Whalen v. Roe, 429 U.S. 589 (1977); Nixon v. Administrator of General Services, 433 U.S. 425 (1977); Ex Parte Jackson, 96 U.S. 727 (1877); Boyd v. United States, 116 U.S. 616 (1886).
[42] The Charter of Fundamental Rights of the European Union, 2000, art. 8.
[43] Justice K.S. Puttaswamy (Retd.) v. Union of India (Privacy), (2017) 10 SCALE 1.

important public concern. Many states have laws that allow the expungement of criminal records in cases of minor offences.[44] Likewise, Mary Bell injunctions are given in the UK to protect the new identity of rehabilitated criminals.[45] These injunctions ensure that the original identity of the rehabilitated criminal and their family remains hidden to protect them from any likely serious harm that may result from revealing their identities to the public. They are named after Mary Flora Bell who had murdered two children when she was eleven years old. The court had granted an injunction to protect not only her, but her daughter as well who could have been victimised by the public for being the child of a murderer.[46]

The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data by OECD also contain similar principles. For example, the "Data Quality Principle" requires that data must be relevant, accurate, complete and up-to-date.[47] Further, the "Individual Participation Principle" allows an individual to request erasure, rectification, completion

[44] The Penal Code of California 1872, § 1203.4; The Texas Code of Criminal Procedure 1965, art. 55.01 – 55.06; Eric Westervelt and Barbara Brosher, *Scrubbing the Past to Give Those With A Criminal Record A Second Chance*, NPR (19 February, 2019), https://www.npr.org/2019/02/19/692322738/scrubbing-the-past-to-give-those-with-a-criminal-record-a-second-chance.

[45] Shamaan Freeman-Powell, *Legal dilemma of granting child killers anonymity*, BBC NEWS (June 11, 2021), https://www.bbc.com/news/uk-47721177.

[46] X (formerly known as Mary Bell) & Y v. News Group Newspapers Ltd. & Ors., [2003] EWHC 1101 (QB).

[47] *OECD Privacy Guidelines* (June 11, 2021), https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

or amendment of personal data.[48] Additionally, the "Principle of Collection Limitation" emphasises upon the consent of the data subject.[49]

The traces of the right to be forgotten can also be found in several instruments. For example, the Canadian Personal Information Protection and Electronic Documents Act, 2000 [*hereinafter* "**PIPEDA**"] provides a right to request correction of personal information.[50] Similarly, the 'Bundesdatenschutzgesetz', Germany's Federal Data Protection Act, 1977, included a right to request the erasure of stored personal data where such storage was impermissible or when the original conditions of data storage were no longer applicable.[51] France's Data Protection Law of 1978, the loi relative à l'informatique, aux fichiers et aux libertés, *i.e.*, "law relating to data processing, files and freedoms", provided a right to correction that also allowed the destruction of data.[52] The Data Protection Act, 1984 of the UK, which was superseded by the 1998 Act and then the 2018 Act, also guaranteed a right to rectification of personal data and a right to erasure.[53] The Privacy Act, 1974 of the USA also guarantees an individual the right to

---

[48] *Id.*
[49] *Id.*
[50] *Draft OPC Position on Online Reputation* (June 11, 2021), https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-on-online-reputation/pos_or_201801/#:~:text=That%20the%20OPC%20proactively%20address,through%20its%20Contributions%20Program%3B%20.
[51] Bundesdatenschutzgesetz 1977, § 4.
[52] Loi relative à l'informatique, aux fichiers et aux libertés 1978, art. 40.
[53] U.K. Data Protection Act 1984, art. 24.

request amendment of their data from the establishments of the executive branch of the federal government.[54]

The CJEU too derived the "right to deindex" in *Google Spain*[55] from the DPD. However, most of these instruments precede the era of big data. They are insufficient to deal with new technology like deepfakes, internet of things, etc. Therefore, the European Union moved towards a new data protection regulation in 2012, and implemented the GDPR in 2018, with the right to be forgotten as one of its pillars.[56] Other jurisdictions have or are in the process of modernising their privacy legislations. For example, in the USA, the State of California passed the California Consumer Privacy Act, 2018 that contains a right to delete personal information and a right to opt-out of processing of personal data.[57] The States of Massachusetts and Nevada have also enacted similar data protection legislations that guarantee the right to delete personal information.[58] The States of New York, Hawaii and Maryland are also poised to enact new consumer privacy legislations. In addition to the right to delete, the proposed New York Privacy Act contains a right of correction as well.[59]

---

[54] 5 U.S.C. § 552 a(d)(2) – (4).
[55] Google Spain SL v. AEPD, Mario Costeja Gonzalez, Case C-131/12, ECLI: EU: C: 2014: 317.
[56] *Fundamental Rights and Citizenship while introducing the right to be forgotten*, OBSERVATIONS OF VIVIANNE REDING, THE EUROPEAN COMMISSIONER FOR JUSTICE; Bennett, *supra* note. 30.
[57] Cal. Consumer Privacy Act 2018, § 1798.105.
[58] Glenn A. Brown, *Consumers' "Right to Delete" under US State Privacy Laws*, THE NAT'L LAW REV. (June 11, 2021), https://www.natlawreview.com/article/consumers-right-to-delete-under-us-state-privacy-laws.
[59] *Id.*

Similarly, Canada is in the process of modernizing its federal privacy legislations, PIPEDA and the Privacy Act, 1983. Its Digital Charter Implementation Act, 2020 would implement the Consumer Privacy Protection Act and the Personal Information and Data Tribunal Act.[60] The Consumer Privacy Protection Act will update PIPEDA which applies to the private sector. The updated law will empower data subjects by enhancing their control over their personal data. It will include a right to request permanent and irreversible deletion of data and a right to request amendment. The UK also has adopted its own General Data Protection Regulation [*hereinafter* "**UK GDPR**"]. The UK GDPR operates under the UK Data Protection Act, 2018. It retains the data protection principles of the European Union's GDPR; it guarantees the right to rectification of incorrect data,[61] the right to request erasure[62] and also the right to object to data processing.[63] Further, it mandates that the data should be relevant, accurate, current and adequate.[64] Additionally, it provides that data can be destroyed if it is no longer required or is excessive for the purpose it was collected.[65]

South Korea has opted for self–regulatory guidelines instead of binding legislation. The Korea Communications Commission issued the

---

[60] *Submission of the Office of the Privacy Commissioner of Canada on Bill C-11, the Digital Charter Implementation Act*, OPC (May 11, 2021), https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_ethi_c11_2105/.
[61] U.K. Data Protection Act 2018, § 46.
[62] *Id.* §§ 47 & 100.
[63] *Id.* § 99.
[64] *Id.* §§ 36, 37, 38, 39, 86 - 91.
[65] *Id.*

Guidelines on the Right to Request Access Restrictions on Personal Internet Postings in 2016.[66] These guidelines enable individuals to request service providers to restrict access to their personal information and to remove information that they cannot delete by themselves. India's Personal Data Protection Bill, 2018, and its revised version, the Personal Data Protection Bill, 2019 also aim to guarantee informational privacy and autonomy to individuals. To that end, they guarantee the right to be forgotten.

In addition to the CJEU ruling in *Google Spain,*[67] the right to be forgotten has also been upheld by national courts. Her Majesty's High Court of Justice in England recognised the right to be forgotten and provided guidance for its application in *NT1 and NT2 v. Google LLC.*[68] The Court directed Google to delist the information concerning the applicant NT2 as per the provisions of the Data Protection Act, 1998. The Court relied on *Google Spain*[69] and Article 29 Working Party Guidelines on Implementation of Google Spain to balance freedom of speech with privacy concerns. It allowed NT2's request since the information pertaining to him had no connection with his current professional and personal life.

---

[66] *KCC takes measures to guarantee "Right to be Forgotten"*, KOREA COMMUNICATIONS COMMISSION, https://www.kcc.go.kr/user.do;jsessionid=u95SDTNn2bk-8xJxpU3DpOa8kxymjESdivHgBfVc.servlet-aihgcldhome10?mode=view&page=E04010000&dc=E04010000&boardId=1058&cp=2&boardSeq=42538.

[67] Google Spain SL v. AEPD, Mario Costeja Gonzalez, Case C-131/12, ECLI: EU: C: 2014: 317.

[68] NT1 and NT2 v. Google LLC, [2018] EWHC 799 (QB).

[69] Google Spain SL v. AEPD, Mario Costeja Gonzalez, Case C-131/12, ECLI: EU: C: 2014: 317.

However, it denied NT1's request as the information in question could play a determinative role in assessing his current professional capabilities.

The Canadian Federal Court also crafted an equivalent remedy in *A.T. v. Globe24h.com*.[70] It directed the Romanian website Globe24h.com to remove Canadian decisions containing personal, financial, medical, and other sensitive information from its website, from search engine caches and to refrain from republishing of such decisions. While these decisions were already available on the Canadian Legal Information Institute's website, these decisions were not indexed by search engines. When Globe24h.com published them, they were indexed and as a result, sensitive information about individuals was displayed as search results. Coupled with this remedy, the Federal Court also awarded damages for the loss of privacy and reputation.

The Supreme Court of India [*hereinafter* "**the Supreme Court**"] in *Justice K.S. Puttaswamy (Retd.) v. Union of India* [*hereinafter* "***Puttaswamy (Privacy)***"][71] observed that the right to be forgotten is concomitant to the right to privacy. The Karnataka High Court too paved the way for the right to be forgotten in *(Name Redacted) v. Registrar General.*[72] Herein, the father of a woman had sought the removal of the woman's name from the digital records of court proceedings she had initiated against a person and from the search results regarding the same as this information was damaging to her current marital relationship and reputation. The High Court acquiesced

[70] A.T. v. Globe24h.com, 2017 FC 114 (Can.).
[71] Justice K.S. Puttaswamy (Retd.) v. Union of India (Privacy), (2017) 10 SCALE 1.
[72] (Name Redacted) v. Registrar General, 2017 SCC OnLine Kar 424.

and recognised a "right to be forgotten" on the lines of foreign jurisdictions. However, the High Court failed to provide any sound basis or any guidance for the implementation of the right. Thereafter, the Delhi High Court in *Zulfiqar Ahman Khan v. Quintillion Business Media (P) Ltd.*[73] held the right to be forgotten as a key aspect of the right to privacy. It observed that both rights were integral to an individual.

The Orissa High Court came to the rescue of a woman whose objectionable pictures and videos were posted on social media.[74] The High Court noted that while strong penal action was available against the accused who had raped and blackmailed the victim, there was no mechanism that could prevent the dissemination of her photos and videos on the internet. Lamenting on the insensitive behaviour on social media towards such victims, the High Court pointed out the need for legislating the "right to be forgotten" as it was not possible in every case for a victim to approach the courts. It further held that it was imperative to recognise the right to be forgotten in such cases lest any accused outrage the modesty of a woman and misuse the same in cyberspace unhindered to harass her.

Recently, the Delhi High Court once again recognised the right to be forgotten of an American citizen by passing an interim order directing online platforms such as Indian Kanoon to block a judgement concerning him from being accessed from search engines.[75] The individual had been acquitted by the Indian courts, yet the judgement which was available on a

[73] Zulfiqar Ahman Khan v. Quintillion Business Media (P) Ltd., 2019 (175) DRJ 660.
[74] Subhranshu Rout v. State of Odisha, 2020 SCC OnLine Ori 878.
[75] Jorawer Singh Mundy v. Union of India, 2021 SCC OnLine Del 2306.

single Google search to any potential employer was hampering his employment prospects causing irreparable harm to him. Therefore, recognising his right to privacy and the right to be forgotten, the Delhi High Court granted him interim relief. Further, the Supreme Court also made certain observations regarding the right to be forgotten in its recent judgement in *Jigya Yadav v. CBSE.* [76] It directed the Central Board of Secondary Education to amend its by-laws and include a mechanism to ensure that corrections or changes may be made in the certificates that it will issue or has already issued. It observed that the new certificates could retain old information with disclaimers, except if the change was effected in the exercise of the right to be forgotten. Notably, it held that the right to control one's identity is a fundamental right.

IV. THE PROPOSED FRAMEWORK FOR THE RIGHT TO BE FORGOTTEN IN INDIA

The Supreme Court in its nine-judge bench decision in *Puttaswamy (Privacy)*[77] upheld the "*fundamental right to privacy*." The judgement marks the beginning of a new era in Indian constitutional law.[78] It places the individual at the heart of fundamental rights jurisprudence and closely interlinks dignity and liberty-based rights. It also clarifies and embeds the "proportionality standard of review" which ensures that fundamental rights are not unduly curtailed.

---

[76] Jigya Yadav v. CBSE, 2021 SCC OnLine SC 415.
[77] Justice K.S. Puttaswamy (Retd.) v. Union of India (Privacy), (2017) 10 SCALE 1.
[78] Shreya Atrey & Gautam Bhatia, *New Beginnings: Indian Rights Jurisprudence After Puttaswamy*, 3(2) U of OxHRH J 1 (2020).

The first step of this standard requires that limitations on fundamental rights must only be imposed to achieve a legitimate purpose. This legitimate purpose must be "rationally connected" to the means adopted for achieving the said purpose. Further, such means must impair the fundamental right in question as minimally as possible. The means also must be necessary and sans any alternatives that may similarly achieve the said purpose with a lesser degree of impairment of the right. The final step requires a contextual balancing of competing interests to ascertain that the cost of impairment is not greater than the benefit of achieving the legitimate purpose. This standard has opened up several possibilities for realizing the transformative character of the Constitution.[79]

Acknowledging the importance of safeguarding informational privacy in the era of big data, the court-mandated steps must be taken to guarantee effective data protection rights. Consequently, a committee chaired by Justice (Retd.) B.N. Srikrishna was constituted to draft a data protection regime for India.[80] The Personal Data Protection Bill, 2018 [*hereinafter* "**2018 PDP Bill**"] was drafted on the recommendation of this committee. The 2018 PDP Bill was debated upon and revised as Personal Data Protection Bill, 2019 [*hereinafter* "**2019 PDP Bill**"]. This 2019 PDP Bill is currently under consideration before a Joint Parliamentary Committee.

---

[79] *Id.*

[80] Justice B.N. Srikrishna Committee, *Report of the Committee on Data Protiection – A Free and Fair Digital Economy Protecting Privacy, Empowering Indians*, MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY (2018).

Several significant changes were made in the new bill including the addition of a right to erasure to supplement the right to be forgotten.

The 2019 PDP Bill is applicable vertically, *i.e.*, to State and its instrumentalities as well as horizontally, *i.e.*, to private entities. It regulates the processing of personal data "*within India, by Indian persons whether corporate or natural, whether in India or otherwise, and those data fiduciaries or data processors outside India in connection to business in India, the systematic activity of offering goods and services to Indian data principals, or profiling of data principals in India*."[81] However, it would not apply to the processing of personal data of Indian data principals outside India by data fiduciaries or data processors outside India.[82] This creates a gap in the regulatory net. For instance, the 2019 PDP Bill will not apply if say a major data fiduciary like Facebook collects and processes or transfers for processing the personal data of an Indian data principal while they are living abroad. If they wish to exercise any of the data protection rights like the right to be forgotten, the only recourse available to them would be an equivalent framework, if any in the foreign jurisdiction, provided it applies to them.

It borrows extensively from the GDPR and recognizes various informational privacy principles such as purpose limitation, limitation on the period for which data can be stored, right of individuals to access data, right to port personal data, privacy by design, etc. It creates a fiduciary relationship between individuals and entities that collect, store, and process

[81] Personal Data Protection Bill 2019, §2.
[82] *Id.*

their personal data. It uses the term "*data principal*"[83] and "*data fiduciary*"[84] to depict this relationship instead of the terms "data subject" and "data controller" used in the GDPR. It imposes a duty of care on data fiduciaries and requires them to process data in a "*fair and reasonable manner*".[85] Data fiduciaries are supposed to ensure that the personal data that is processed is complete, accurate and is not misleading or outdated.[86] They must not retain the data longer than necessary for the purpose for which it was collected unless legally bound to do so.[87] Depending on the volume and sensitivity of the data, the 2019 PDP Bill creates a special class of data fiduciaries termed "*significant data fiduciaries*".[88] They are subject to higher penalties in case of violation of the provisions of the proposed bill.

The consent of the data principal is central to its framework. Barring certain exceptions, personal data can only be processed on the basis of "*free, informed, specific and clear consent of the data principal*."[89] The consent must be capable of being withdrawn and has to be taken before processing.[90] Consent requirements are more stringent for the processing of sensitive personal data.[91] Further, the 2019 PDP Bill creates the Data Protection Authority of India [*hereinafter* "**DPAI**"] to ensure enforcement

[83] *Id.* § 3(14).
[84] *Id.* § 3(13).
[85] *Id.* § 4.
[86] Personal Data Protection Bill 2019 § 8.
[87] Personal Data Protection Bill 2019 § 9.
[88] *Id.* § 36.
[89] *Id.* § 11.
[90] *Id.*
[91] *Id.* § 11(3).

of its provisions.[92] It confers extensive powers on the DPAI, such as the power to call for information, search and seizure, etc.[93] The adjudicatory division of DPAI imposes penalties for violation of compliance requirements and offences under the proposed bill.[94]

In addition to the right to be forgotten[95] and the right to erasure,[96] the 2019 PDP Bill also guarantees a right to correction of incorrect or misleading data,[97] completion of incomplete data,[98] and updating of outdated data.[99] The right to be forgotten enables the data principal to request the DPAI to restrict or prevent the continued disclosure of his data by a data fiduciary only on the three specified grounds. *First*, the disclosure of data has served the purpose for which it was collected and is no longer necessary for that purpose. *Second*, the consent has been withdrawn by the data principal for the disclosure of data that was collected and processed with the consent of the data principal. *Third*, when the disclosure is contrary to the provisions of any legislation in force. Further, the data principal must establish that his right to restrict disclosure overrides the freedom of speech, expression, and information of others. Hence creating a presumption in favour of freedom of speech and expression.

---

[92] *Id.* § 41.
[93] *Id.* §§ 51-55.
[94] *Id.* §§ 57-66.
[95] *Id.* § 20.
[96] *Id.* § 18.
[97] *Id.*
[98] *Id.*
[99] *Id.*

While considering such a request, the Adjudicating Officer of the DPAI is required to take into account the sensitivity of the data, the role of the data principal in public life, the scale of disclosure, the degree of accessibility sought to be restricted and the activities of the data fiduciary and whether they would be significantly impeded. An appeal lies from the decision of the Adjudicating Officer to the Appellate Tribunal and thereafter to the Supreme Court. Unlike the GDPR which allows data subjects to request the data controllers directly, the 2019 PDP Bill has avoided conferring the responsibility of balancing speech and privacy on private entities. However, the DPAI under the 2019 PDP Bill is no longer independent and it is doubtful if it would not be biased when the request is directed to the government or its instrumentalities as data fiduciaries.[100]

The right to erasure on the other hand is only available when the data is no longer necessary for the purpose for which it was collected.[101] The requests for erasure, correction, completion and updating can be made directly to the data fiduciary. If the data fiduciary accepts the request of erasure, it must notify all other entities to whom the disclosure was made regarding such erasure. If it refuses such a request, then it has to offer reasonable justifications for the same.[102] Failure to do so can attract a penalty of up to INR 5,000 (five thousand) per day with a maximum cap of

[100] Lakshya Sharma and Siddharth Panda, *Into the Orwellian Dystopia: A Comparative Analysis of Personal Data Protection Bill 2019 vis-à-vis Indian Privacy Jurisprudence,* 7(2) NLUJ L. REV. 1, 27(2021).
[101] Personal Data Protection Bill, 2019 § 18.
[102] *Id.* § 21(4).

INR 10,00,000 (ten lakh) for significant data fiduciaries and INR 5,00,000 (five lakh) for other data fiduciaries.[103] There is no specific provision for appeal. However, the general right to complaint to the DPAI for contravention of the provisions of the 2019 PDP Bill[104] is available to the data principal in case of refusal. On receiving such a complaint, the DPAI would appoint an Inquiry Officer. Based on the report submitted by the Inquiry Officer and after hearing the data fiduciary, the DPAI can give appropriate directions in writing.[105] The data principal can appeal against such an order to the Appellate Tribunal.[106]

It is questionable whether the current framework would strike an appropriate balance with freedom of speech and expression and be constitutionally compatible. Apart from the lack of independence of DPAI, there are other issues that plague this framework. For example, the Adjudicating Officer has hardly been given any guidance regarding the application of grounds on which the right to be forgotten can be availed. The factors provided leave a lot of room for discretion and need clarification. There is no distinction between data posted by the data principal himself and data posted by other people about the data principal in either of the provisions. This should be a very important factor in considering a request regarding these rights as the latter would implicate the right to free speech of others while the former would only implicate their right to access the information. The right to erasure can be handy in other

---

[103] *Id.* § 58.
[104] *Id.* § 53.
[105] *Id.* § 54.
[106] *Id.* § 72.

situations like revenge porn and should have been drafted to encompass such a situation. The present provision seems superfluous considering that the data fiduciaries are anyway not allowed to retain the data beyond the period necessary for the purpose it was collected.[107] If they do so, the DPAI may suo motu or on a complaint received by it, initiate an inquiry and take action against them.[108] Further, for non-compliance with this requirement, they would be subject to a penalty of up to INR 15,00,00,000 (fifteen crores) or four per cent of their total worldwide turnover of the preceding financial year, whichever is higher.[109] Further, a data principal can also complain to the DPAI and seek compensation from the data fiduciary if the data principal suffers harm as a result of contravention of this requirement.[110]

Moreover, the 2019 PDP Bill does not specify what remedies may be given to restrict disclosure of personal data in the context of the right to be forgotten. Is only delisting/deindexing permitted or remedies like de-ranking may be given? It also does not clarify if takedown of information from the source website can be done to restrict disclosure. Further, it also does not leave room for other remedies like flagging of information as unreliable or under-review which may sometimes be enough to prevent the harm to the data principal or could be used as an interim relief while the

[107] *Id.* § 9.
[108] *Id.* §§ 53(1) (b) – 54.
[109] *Id.* § 57(2).
[110] *Id.* § 64.

request for the right to be forgotten or erasure, completion, correction or updating is pending.

The following sections explore how competing rights are balanced in India and offer suggestions for designing a constitutionally compatible right to be forgotten in India.

V. RECONCILING FREEDOM OF SPEECH AND EXPRESSION AND PRIVACY IN THE CONTEXT OF THE RIGHT TO BE FORGOTTEN

The Constitution of India is a "transformative document".[111] The provisions of Part III of the Constitution are interpreted as a whole and in a progressive manner.[112] There are some rights like freedom of religion which have been subjected to other rights[113] and there are some rights that have been expressly qualified.[114] However, there is no hierarchy of rights in the Constitution. Nor is precedence given to one constitutional value over the other.

When two rights compete against one another, there is no clear winner. The competing rights are contextually balanced against each other to determine the outcome. For instance, in the case of *Mr X. v. Hospital Z,*[115] the Supreme Court was called upon to balance the right to privacy of an HIV patient against the right to life and health of his fiancée. Herein, a

---

[111] GAUTAM BHATIA, THE TRANSFORMATIVE CONSTITUTION: A RADICAL BIOGRAPHY IN NINE ACTS (HarperCollins India 2019).
[112] Maneka Gandhi v. Union of India, AIR 1978 SC 597.
[113] INDIAN CONST. art. 25.
[114] *Id.* art. 19, art. 25.
[115] Mr X. v. Hospital Z, AIR 1999 SC 495.

doctor had disclosed the appellant's HIV positive status to his fiancée which ultimately led to the cancellation of his marriage. The Supreme Court acknowledged that the appellant had a right to privacy and the doctor owed a duty of confidentiality to his patient. However, in the given circumstances his fiancée had a greater interest in knowing this information.

Similarly, in *in re Noise Pollution and Restricting Use of Loudspeakers,*[116] the Supreme Court balanced the right to life and a clean environment under Article 21 of the Constitution against freedom of speech and expression. Once again, the Supreme Court contextually balanced the conflicting rights and observed that while there was freedom of speech and expression, the same was not absolute. Nobody had the right to engage in "*aural aggression*" as others had an equal right not to be compelled to listen and enjoy a peaceful life. The harmful effects of noise on health also tilted the balance in favour of the right to a clean, pollution-free environment in this case.

Hate speech and defamation jurisprudence inevitably involve a balancing exercise between freedom of speech and dignity.[117] The requirement of reasonability for restrictions on Article 19 freedoms has always required proportionality and therefore contextual balancing. Therefore, while the landmark cases of *Modern Dental College*[118] and *Puttaswamy (Privacy)*[119] formally introduced the proportionality standard in

[116] In re Noise Pollution and Restricting Use of Loudspeakers, AIR 2005 SC 3136.
[117] Subramanian Swamy v. Union of India, (2016) 7 SCC 221.
[118] Modern Dental College and Research Centre v. State of Madhya Pradesh, (2016) 7 SCC 353.
[119] Justice K.S. Puttaswamy (Retd.) v. Union of India (Privacy), (2017) 10 SCALE 1.

our constitutional jurisprudence for testing limitations on rights, it was never an alien concept. For instance, in *State of Madras v. V.G. Row*,[120] a case regarding freedom of association, the Supreme Court pointed out the link between the reasonableness of a restriction and proportionality. It observed that while assessing the reasonability of a restriction, it would consider the nature of the right in question and the purpose of the restriction imposed. Further, it would consider the extent and urgency of the mischief sought to be remedied, *i.e.*, the necessity. Lastly, it would examine whether the restriction was proportionate as per the prevailing circumstances at the time.

Freedom of speech and expression is a precious right in India considering its history during the freedom movement. And while free speech jurisprudence in India borrows heavily from the First Amendment jurisprudence, it has never been regarded as a superior right. As discussed above, it does not automatically trump other fundamental rights in case of a conflict. Even in the USA, scholars have been clamouring for reading the First Amendment with the Thirteenth and Fourteenth Amendment, particularly in the context of hate speech.[121] In contrast, the requirement of reasonableness under Article 19 closely resembles the balancing exercise undertaken by the Supreme Court of Canada in cases like *Oakes*,[122] *Hill*[123]

---

[120] State of Madras v. V.G. Row, AIR 1952 SC 196.

[121] RICHARD DELGADO AND JEAN STEFANCIC, MUST WE DEFEND NAZIS? WHY THE FIRST AMENDMENT SHOULD NOT PROTECT HATE SPEECH SUPREMACY (NYU Press 2018).

[122] R v. Oakes, [1986] 1 S.C.R. 103 (Can.).

[123] Hill v. Church of Scientology, [1995] 2 S.C.R. 1130 (Can.).

and Dagenais,[124] the European Court of Human Rights in *Axel Springer*,[125] the House of Lords in *Campbell*,[126] and the South African Constitutional Court in *NM v. Smith.*[127]

The underlying principle in this reconciliatory exercise is that of proportionality. Both sets of conflicting rights are defined in the light of each other, as neither is considered superior to the other.[128] In fact, it is understood that each of these rights informs and is informed by the other. Under this exercise, it is first determined that the limitation is imposed through law, and that it is for a legitimate interest since a fundamental right is at stake. Thereafter, it is seen whether the limitation imposed on one right is necessary in order to prevent a real and substantial risk to the other and that reasonably available alternative measures would not prevent the risk. And finally, it is seen that in the given context the salutary effects of the limitation in safeguarding one fundamental right should outweigh the deleterious effects of limiting the other.

Likewise, while testing the reasonability of restrictions on Article 19(1)(a) of the Constitution, the first stage is to determine whether the restriction has been imposed by a law. The next is to see if the limitation has been imposed on the basis of one of the grounds mentioned in Article 19(2), a legitimate state interest. The rational nexus of the limitation with one of the mentioned grounds also entails the necessity of the restriction

---

[124] Dagenais v. Canadian broadcasting Corp., [1994] 3 S.C.R. 835.
[125] Axel Springer AG v. Germany, 39954/08 [2012] ECHR 227 (7 February 2012).
[126] Campbell v. MGN Ltd., [2004] UKHL 22.
[127] NM v. Smith, [2007] ZACC 6.
[128] Subramanian Swamy v. Union of India, (2016) 7 SCC 221.

to achieve the aim mentioned in Article 19(2) and the lack of equally effective alternative means. And finally, the elements of proximity and proportionality require that the limitation must be narrowly tailored to achieve the legitimate aim and must not be an overbroad restriction. For instance, in *Romesh Thappar v. State of Madras*,[129] Section 9(1-A) the Madras Maintenance of Public Order Act was struck down as it did not have a rational nexus with any of the legitimate aims mentioned in Article 19(2) and was overbroad. Similarly, in *Shreya Singhal v. Union of India*,[130] Section 66A of the Information Technology Act, 2000 was struck down as overbroad, vague, arbitrary and disproportionate. Recently, in *Anuradha Bhasin v. Union of India*,[131] the Supreme Court reiterated that orders for internet shutdowns must comply with the proportionality standard.

Restrictions on the right to privacy also need to pass the touchstone of proportionality. The standard has been applied since *Puttaswamy (Privacy)*[132] in various decisions like *Puttaswamy (Aadhar)*,[133] *Navtej Singh Johar*[134] and *Joseph Shine*[135] to test the validity of restrictions on privacy-dignity-autonomy. As the right to be forgotten represents privacy-dignity-autonomy interests, it can be restricted only as per the proportionality standard.

---

[129] Romesh Thappar v. State of Madras, AIR 1950 SC 124.
[130] Shreya Singhal v. Union of India, AIR 2015 SC 1523.
[131] Anuradha Bhasin v. Union of India, 2020 SCC OnLine SC 1725.
[132] Justice K.S. Puttaswamy (Retd.) v. Union of India (Privacy), (2017) 10 SCALE 1.
[133] Justice K.S. Puttaswamy v. Union of India (Aadhar), (2019) 1 SCC 1.
[134] Navtej Singh Johar v. Union of India, AIR 2018 SC 4321.
[135] Joseph Shine v. Union of India, (2019) 3 SCC 39.

Hence, while balancing both freedom of speech and expression and privacy-dignity-autonomy in the context of the right to be forgotten, both sets of rights would have to be informed by each other. They would have to be read in a manner that minimally impairs each right while simultaneously effectively safeguarding both. This is clearly a delicate task and requires sufficient guidance. In this process, the first step should be to regard both sets of rights at equal footing since the Constitution does not give preference to either, nor does it prefer liberty over dignity or vice-versa. Further, both sets of rights are liberty as well as dignity based and are correlated.

Protecting both sets of rights is a legitimate state interest, and since Part III of the Constitution is read as a whole, both sets of rights should be harmoniously interpreted. At the next stage of necessity, restrictions imposed on freedom of expression and access to information on the one hand, and privacy-dignity-autonomy on the other hand, must be examined for their effectiveness and need. If there are equally effective, less restrictive measures available, then those should be resorted to. Thus, when de-ranking of information in search results can suffice, delisting should not be given as a remedy. On the other hand, there may be cases of revenge porn or cases involving information about a minor that warrant the remedy of erasure of the information from the source. At the same time exceptions meant to ensure freedom of speech and expression like "journalistic purposes"[136] must be clearly defined through an inclusive list to prevent an

[136] Personal Data Protection Bill 2019 §36.

overbroad interpretation. Particularly, the government's power to grant such exemptions to its agencies[137] must be limited.

Finally, while examining the proportionality, it must be ensured that both the right to be forgotten and the exceptions to safeguard speech and expression are tailored narrowly to effectively safeguard the underlying rights. Taking a cue from these principles, the next section offers certain suggestions regarding drafting a constitutionally compatible "right to be forgotten" provision.

VI. SUGGESTIONS AND CONCLUSION

To reconcile freedom of speech and expression with privacy-dignity-autonomy in the context of the right to be forgotten, the author recommends the following amendments. *First*, there shouldn't be separate provisions and procedures for the right to be forgotten and erasure, correction, completion and updating.

The provision for the right to be forgotten must offer a combination of catalogue and standards. The catalogue should enlist fact situations with corresponding remedies to be granted as a rule. For example, in cases involving intimate photos or videos, the remedy of irretrievable erasure from the source and other links should be given as a rule. Similarly, matters pertaining to marital relationships or discords may be delisted after a reasonable period of three to five years. This catalogue can be revisited from time to time as jurisprudence develops. If the data

[137] *Id.* § 37.

principal's case falls within the catalogue, he should be allowed to approach the data fiduciary directly with a mechanism of appeal to the Appellate Tribunal in case of refusal.

The rest of the requests by should be determined according to standards. The data principal must not bear the burden of proving that his privacy-dignity-autonomy interest overrides the free speech and access to information rights of others. This should, however, be a determinative factor during balancing. It should be seen that who is has authored the information. If the author was the data principal then the balance should shift in favour of the right to be forgotten; if however, the information was posted by others, it should shift in favour of freedom of speech. It should also be seen if the data principal was a minor when the information was posted; this should shift the balance towards the right to be forgotten. Next, the newsworthiness of the data must be assessed having regard to factors such as time elapsed, the sensitivity of the information, the role of the data principal in public life and the relevance of that information to his public life. And if the information pertains to his private life, whether the data principal had deliberately courted publicity by exposing his private life or if that information is associated with his role in public life despite its sensitivity.

As a general rule, de-ranking relevant search results should be the preferred remedy unless making them inconspicuous cannot prevent harm to the data principal. In those cases, delisting may be granted as a remedy as it would further limit access to the information by removing relevant links from the search results. The remedy of erasure and takedown from

the source must only be granted in exceptional circumstances when there are compelling privacy-dignity-autonomy interests. Additionally, when a request if pending, the information can be flagged as under review so that those accessing it do not rely upon it. Also, when a request is denied for exceptions like "journalistic purposes", then too the information can be flagged to indicate so.

These requests should be heard by a DPAI panel consisting of a technical and a judicial member having significant experience with a mechanism of appeal to the Appellate Tribunal. Further, the independence of the DPAI must be ensured by modifying the process of composition and appointment. The DPAI members must be selected by a panel consisting of representatives of the government, industry, and the judiciary to counterbalance any influence they may exercise. The term of five years for the members must be a rule and members should be removed only under the specified grounds.

It is imperative that freedom of speech and expression is not impeded and that the right to be forgotten does not remain a paper tiger. Both sets of rights are valuable and must be zealously guarded in the era of big data. A narrowly tailored right to be forgotten would not only ensure the privacy-dignity-autonomy of individuals but also prevent the chilling effect on speech on the internet due to lack of informational autonomy. The author believes that the above suggestions may be helpful in achieving this objective.

NLUJ Law Review

Yash Sinha, *Why a Cap on Work-Hours gets congealed into a Constitutional Threshold*, 8(1) NLUJ L. REV. 40 (2021).

WHY A CAP ON WORK-HOURS GETS CONGEALED INTO A CONSTITUTIONAL THRESHOLD

*Yash Sinha**

ABSTRACT

The act of relaxing the limit on factory working-hours by a few Indian states in 2020 was akin to a constitutional flyby. Furthermore, there was no parallel increment in minimum wages. Both phenomena involve a dilution of statutes under Part IV of the Constitution of India. Both are, however, fortuitously barred by three unique constitutional prohibitions.

First of these is proposed to be a 'constitutional transference'. Upon fulfilment, certain positive obligations espoused under Part IV come under the aegis of negative obligations imposed on the State in Part III. Diminishing the former then impermissibly violates Part III. Both work hours and minimum wages are obligations of this mutable nature. Secondly and alternatively, the emerging principle of non-retrogression completely bars putting workers in inferior circumstances than they currently suffer.

In any case, there exists another two-pronged bar, wholly rooted in concurrent-federalism. Both, alternatively, disfavour the acts of Indian states in this

* The author is a 2019 graduate of National Law School of India University and currently practicing as an Advocate in New Delhi. He may be contacted at **yash95sinha@gmail.com**.

instance. The 'exhaustive field' test prioritises a law from that unit of federation which evinces the intention to govern the concerned legislative subject. Whereas, the 'denial of rights' test disables the concurrent powers when one unit of the federation attempts to denature laws enacted by its complement.

Hence, the states' objective to increase working hours without the guarantee of a proportionate recompense, was most definitively under a constitutional interdict.

TABLE OF CONTENTS

I. INTRODUCTION

The Constitution of India [*hereinafter* "**the Constitution**"] had envisaged a central-state collaboration in regulating labour standards by placing it in the Concurrent List.[138] One such legislation is the Factories Act, 1948 [*hereinafter* "**the Act**"].[139] Several Indian states invoked powers conferred by Section 5[140] of the Act to undertake nothing less than a fundamental overhaul of workers' rights, in the name of recalibrating their working hours. The amendments involved suspension and modification of Sections 51, 54, 55, and 56 of the Act, respectively dealing with working hours per day, per week, its spread within a day, and the duration of daily intervals.[141] These were introduced in the backdrop of labour shortages as a consequence of inter-state labour migration and a cap on the number of people at a given place due to the pandemic, adversely affecting industry productivity.[142] To make up for the cumulative effect of the two factors, the industries were afforded an opportunity for extracting labour for a relatively prolonged period of time.[143] Ostensibly, this may appear to be constitutionally permissible, given the available legal competence and no perceivable bar on reducing working hours *per se*.

---

138 INDIA CONST., Schedule VII, List III, *Concurrent List*.
139 The Factories Act, 1948, No. 63, Acts of Parliament, 1948.
140 See *Id.* § 5.
141 See *Id.* §§ 51, 54-56.
142 K.R. Shyam Sundar, *Factory Workers Can Now Legally Be Asked to Work 12-Hour Shifts: How Will this Change Things*, THE WIRE (April 27, 2020), https://thewire.in/labour/factory-workers-12-hour-shifts.
143 *Id.*

However, procedural competence and the absence of substantive legal bars are not the only means of testing an action's constitutionality. Both constitutional and common law come with certain safeguards, of which three are pertinent to this scenario. *Firstly*, this is explicitly precluded by the prevailing Indian jurisprudence around labour laws. *Secondly*, common law envisages another prohibition through the non-retrogression principle, for rights demanding a progressive realisation. *Thirdly*, prevailing jurisprudence on federalism disables legislative powers when one of its units departs from constitutional objectives.

This paper argues that these moves by the states could not have stood these standing legal tests.

Section II of this paper analyses these state notifications singularly within the paradigm of Parts III-IV of the Constitution, through four constituent parts. Section II(A) gives a brief description of the Supreme Court of India's [*hereinafter* "**the Supreme Court**"] reasoning in *Gujarat Mazdoor Sabha v. State of Gujarat* [*hereinafter* "***Gujarat Mazdoor Sabha***"].[144] Herein, the Supreme Court had agreeably struck down a notification for one of the states, albeit by way of an incomplete *ratio*.[145] The following Section II(B) shall reveal the significant gaps in both the *ratio* and its underlying premises insofar as the decision criminally disregards the role of 'wage rate' in labour rights. Section II(C) will build upon the foundation laid down in the preceding sub-section and will demonstrate that the

[144] Gujarat Mazdoor Sabha & Anr. v. State of Gujarat, 2020 10 SCC 459 ("***Gujarat Mazdoor Sabha***").
[145] *See* discussion *infra* Section ll.

notifications tacitly permitted a notional theft of minimum wages. It argues that the prescription of a minimum wages always takes into account the permissible cap on maximum work hours, and that an increment in the latter without a concomitant increment in the former allows for a *de facto* deduction in minimum wages. Section II(D) reveals how both the Parts function on a principle of mutual transference. That is, a fulfilled directive principle by the government becomes a secured fundamental right of the citizen. The phrasing of Article 23 of the Constitution is deliberately open ended so that it could attach itself to a fulfilled directive principle. The latter, then, comes under the heightened security that Part III comes with. The Section attempts to draw this link through the jurisprudence on minimum wages, a notional deduction of which is taking place in the case at hand.

Alternatively, Section III argues that the notifications in this case were precluded by the emerging 'non-retrogression' principle. Section III(A) describes the sources for this principle, as they exist in the form of legal texts. Section III(B) describes the theoretical underpinnings of the principle as it (exclusively) developed and applied in the U.S. Constitutional jurisprudence. It focuses on the crux of the principle, which is its running prohibition on the State to dilute or retract any previous act of it that had enhanced the citizens' constitutional rights. Eventually, Section III(C) asserts that Indian constitutional law in general and Indian constitutional-labour jurisprudence in particular is fertile ground for the principle's application. It argues that the Indian constitutional objective of 'attaining' the realisation of enumerated rights is meaningless if the government has

the power to later retract it. In avoiding such an absurd interpretation of constitutional law, the non-retrogression principle should be applied to strike down actions such as the concerned notifications.

Section IV is composed of the last alternative argument in this regard. It proposes that India's quasi-federation is a competitive marketplace for legislative ideas. A vertically-federal unit may only utilise the concurrent jurisdiction to enhance the prevailing laws. The negation/enhancement may be either quantitative or qualitative. Section IV(A) covers the quantitative test of 'occupying a field'. It argues that the Centre had appropriated the subject of working conditions[146] to itself by evolving multiple laws. Alternatively, Section IV(B) argues that the states were precluded in their actions by the qualitative 'denial of rights' test. This looks at whether the act of one federal unit obliterates the other unit's rights-based initiative, regardless of which one has the greater legal infrastructure. By both measures, the Section attempts to establish a federal-legal bar on the states in this case.

For the sake of fluency and convenience, states would imply both the state executives and the respective legislatures throughout the paper, unless explicitly mentioned otherwise. The same is to be assumed for the terms Union/Centre. The term 'amendments' shall be taken to reflect both, an executive's exercise of delegated powers and acts of legislatures.[147]

---

[146] INDIA CONST., Schedule VII, List III, Item 24.
[147] INDIA CONST., art. 13, cl. 3.

II. CONSTITUTIONAL 'TRANSFERENCE' REVEALS THESE NOTIFICATIONS TO BE VIOLATING A FUNDAMENTAL RIGHT

At least eight Indian state executive branches went ahead to exercise the powers under Section 5 of the Act to increase the working hours on a daily and weekly basis.[148] Effectively, in most of the states, the new cap on daily work hours was 12 hours as opposed to the previous limit of 9 hours.[149] Furthermore, the new cap on the total daily spread-over of working hours were slated to be increased from the previous limit of 10.5 to 13 hours (average).[150] None of this was accompanied by any proportionate increment in the minimum wage floors. The notifications, then, effectively provided a platform to factories for a notional deduction in minimum wages. This goes against the constitutional intention of providing a framework wherein a worker shall not have to sacrifice her rights to earn a livelihood.[151]

This Section argues that the Constitution bars such notional deductions. It is proposed that the obligation to provide the same is captured by Part IV. However, once provided, it stands 'transferred' to Part III and any subtraction from it amounts to violating Part III in general, and Article 23 in particular.

---

[148] Anya Bharat Ram, *Relaxation of labour laws across states*, PRS LEGISLATIVE RESEARCH (May 12, 2020), https://www.prsindia.org/theprsblog/relaxation-of-labour-laws-across-states. ("**Anya**")
[149] *Id.*
[150] *Id.*
[151] 2B. SHIVA RAO, THE FRAMING OF INDIA'S CONSTITUTION 100 (1966).

Indian states in their formulation of minimum wage-floors base it on a day-to-day parameter.[152] This is because this parameter is essentially tied with 'consumption units', components of which (such as daily calorific needs) are traditionally calculated for a day.[153] Forced labour comes about when there may be a notional wage deduction, such as when the same wages are not adjusted for inflation.[154] The same deduction comes about when the duration of a 'day' is increased, keeping wages *per* day stagnant.

A. THE SUPREME COURT'S ROUTE OF INVALIDATING THE NOTIFICATION(S)

Before delving deeper into the relevant arguments, it is pertinent to note why the Respondent's, *i.e.*, the State of Gujarat's, notification was struck down in *Gujarat Mazdoor Sabha*. The two Petitioners included trade unions belonging to both the federal levels. In its written submissions, the Respondent admitted that the object of the notifications was not to gear up private production, but merely to push factories towards meeting their financial break-even points.[155]

Predominantly, the discussion in *Gujarat Mazdoor Sabha* revolved around the expanse of the phrase 'public emergency', which is a pre-

---

[152] IndiaSpend Team, *New formula for minimum wage in India could double incomes – but only if implemented right*, SCROLL.IN (May 6, 2019), https://scroll.in/article/915456/new-formula-for-minimum-wage-in-india-could-double-incomes-but-only-if-implemented-right; *see also* The Minimum Wages Act, 1948, No. 11, Acts of Parliament, 1948, § 3.
[153] Anya, *supra* note 148.
[154] P.U.D.R. & Ors. v. Union of India & Ors., 1982 3 SCC 235, ¶ 14 ("***PUDR***").
[155] *Gujarat Mazdoor Sabha*, *supra* note 144, ¶ 29.

condition for invoking the powers under Section 5.[156] The Supreme Court simply deployed the admitted position of the Respondent of helping the employers as a vehicle to invalidate its notification. It stated that this distinguished the case from *Pfizer Private Limited, Bombay v. Workmen*,[157] which would have otherwise favoured the Respondent. Therein, the aim of expanding the employer's entitlements was to gear up production that the country needed; it was not to reach a financial break-even. The Supreme Court further stated that unlike the state-imposed public emergency at hand, that case was a private dispute between parties.

The Supreme Court then stated that the present case was not even sufficient to invite the state-imposed emergency. It applied the concentric-circle test espoused in *Dr. Ram Manohar Lohia v. State of Bihar & Ors.*[158] to the Explanation in Section 5. It held the COVID-19 induced financial stress to be outside the smallest ring of 'state-security'.[159] This, therefore, removed the very foundation of a 'public emergency' use of the provision. This significant factor, alongside increased fatigue on the worker due to prolonged working hours,[160] violated Articles 21 and 23 of the Constitution, according to the Supreme Court.[161]

---

[156] The Factories Act, 1948, No. 63, Acts of Parliament, 1948, § 5.
[157] Pfizer Private Limited, Bombay v. Workmen, AIR 1963 SC 1103.
[158] Dr. Ram Manohar Lohia v. State of Bihar & Ors., 1966 SCR (1) 709.
[159] *Gujarat Mazdoor Sabha*, *supra* note 144, ¶ 30.
[160] *Id.*, ¶¶ 40, 41, 47; Y.A. Mamarde v. Authority, 1972 2 SCC 108.
[161] INDIA CONST., art. 21, 23.

B. THE DISCONTENTS OF GUJARAT MAZDOOR SABHA

With great deference, it is submitted that the Supreme Court failed to authoritatively denounce the legalisation of paying below minimum wages. It is pertinent to note that when the Respondent state herein was an exception amongst the notifying states insofar, it explicitly alluded to extra wages for the added work-hours. If INR 80 was the floor rate for 8 work hours, it would become INR 120 in the case of 12 work hours. The state, like others, had been specifying rates on a day-based parameter till this point.[162] That is, the workers were to be awarded wages for the extra hours worked, at the same wage per hour rate as earlier.

However, it is submitted that longer work hours demand an increment in wage rate, and not a compensation at the rate as existed previously. *A priori*, this inordinate proportionality between work hours and minimum wages is captured by available empirical literature.

Firstly, there is the factor of exponentially increased efforts during the later work hours of the entire duration. The period of work is not a continuum of the same circumstances, but an arc of gradually depleting efficiency in her devoted efforts towards work.[163] To provide the same level of labour productivity as earlier in the day, a worker needs to put in a

---

[162] Ministry of Labour and Employment, Government of India, Response to Lok Sabha Unstarred Question No. 1118, (December 17, 2018), http://164.100.24.220/loksabhaquestions/annex/16/AU1118.pdf.

[163] Sabina Kołodziej & Mariusz Ligarski, *The Influence of Physical Fatigue on Work on a Production Line*, 20(3) ACTA TECHNOLOGICA AGRICULTURAE 63, 64-68 (2017).

relatively higher effort as the clock-out time approaches.[164] This is a consequence of tapering efficiency.[165] This is to be read with the Act permitting shift working,[166] which compounds the implications in a case such as this: night-shift workers fighting off of their natural circadian rhythm shall have prolonged their internal biological conflict.[167]

Secondly, it is proposed that the exacerbated post-work fatigue requires recompense at a higher rate. Longer working hours are mostly left to the will of the worker in the form of an electable overtime option. When longer hours are imposed as mandatory, the amount devoted to sleep and spent on leisure, decreases.[168]

The available literature suggests the efficiency-wage hypothesis works towards mitigating or precluding damage by both the above factors.[169] This hypothesis stipulates that the productivity of workers

---

[164] Christopher M. Barnes, *The Ideal Work Schedule, as Determined by Circadian Rhythms*, HARVARD BUSINESS REVIEW (January 28, 2015), https://hbr.org/2015/01/the-ideal-work-schedule-as-determined-by-circadian-rhythms.

[165] India Today Web Desk, *Henry Ford started the 40-hour workweek but the reason will surprise you*, INDIA TODAY (July 27, 2017), https://www.indiatoday.in/education-today/gk-current-affairs/story/40-hour-workweek-henry-ford-1026067-2017-07-27.

[166] The Factories Act, 1948, No. 63, Acts of Parliament, 1948, § 2(r).

[167] Mia Son et al., *Effects of long working hours and the night shift on severe sleepiness among workers with 12-hour shift systems for 5 to 7 consecutive days in the automobile factories of Korea*, 17 JOURNAL OF SLEEP RESEARCH 385, 387-394 (2008).

[168] Sungjin Park et al., *The negative impact of long working hours on mental health in young Korean workers*, 15(8) PUBLIC LIBRARY OF OPEN SCIENCE ONE (2020); Kenji Iwasaki et al., *Effect of Working Hours on Biological Functions related to Cardiovascular System among Salesmen Machinery Manufacturing Company*, 37(1) INDUSTRIAL HEALTH 361, 364-366 (1999).

[169] Maarten D.C. Immink and Fernando E. Viteri, *Energy intake and productivity of Guatemalan sugarcane cutters: An empirical test of the efficiency wage hypothesis part II*, 9(2) JOURNAL OF DEVELOPMENT ECONOMICS 273, 275-278, 280-287 (1981).

proportionately increases with the wage increment.[170] This has been factored in by the Supreme Court for minimum wage disputes.[171]

Thirdly, there exists an undeniable link between calories consumed and minimum wages paid when it comes to the lowest economic quintile of the working class.[172] Minimum wages push the entire household of a worker towards the (biologically) required calorific consumption.[173] The sensitivity of this link between work-hours and calories consumed is extremely high.[174] When the work-hours decrease, such households' calorie consumption decreases inordinately.[175] That is as good as a wage deduction.

It is in this light that the Supreme Court's previous reading of the public policy as necessitating complete social, physical and mental health in contractual hires must be interpreted.[176] Aligned cumulatively, the three factors unfailingly denote hours to be the most significant unit for gauging spent labour. Most implicative in this regard is its mention as the lone metric by the two relevant statutes at certain places.[177]

---

[170] *Id.*
[171] Express Newspapers v. Union of India, AIR 1958 SC 578.
[172] Mike Palazzolo & Adithya Pattabhiramaiah, *The Minimum Wage and Consumer Nutrition*, RESEARCH PAPER 2021 JOURNAL OF MARKETING RESEARCH, 20, 70-71, (February, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3547832 ("**Palazzolo**"); Kathryn L. Clark, *Minimum wages and healthy diet*, 38(3) CONTEMPORARY ECONOMIC POLICY 546, 559 (2020); Lindsay Beck et al., *Low-income workers' perceptions of wages, food acquisition, and well-being*, 9(5) TRANSLATIONAL BEHAVIOURAL MEDICINE 942, 949-951 (2019).
[173] Palazzolo, *supra* note 172.
[174] *Id.* at 29-30.
[175] *Id.* at 70-71.
[176] C.E.S.C. Ltd. Etc. v. Subhash Chandra Bose & Ors., 1992 1 SCC 441 , ¶¶ 31-33.
[177] *See* The Factories Act, 1948, No. 63, Acts of Parliament, 1948, §§ 51, 53, 54, 55, 56, 57(b), 59; The Minimum Wages Act, 1948, No 11, Acts of Parliament, 1948, §§ 13, 14.

This aligns with the larger welfare objective to evolve from economics-driven quantum of wages to one based on 'entitlement'. This is so because if left to the former, the employer may be dictated by demand-supply factors to lower the wages disbursed to the weakest of working classes.[178] This makes it possible that essential commodities remain ample in supply, but the workers' access to those becomes minimal.[179] Added to this, the Indian constitutional law had desired a transformative journey graduating from minimum to fair wages, with living wages as the ultimate objective in floor limits of payments.[180] Executive orders by Indian states, it is submitted, were akin to placing the cart before the horse.

C. DISPROPORTIONALITY IN REAL TERMS: NOTIONAL THEFT OF MINIMUM WAGES

In terms of economic dignity, *Gujarat Mazdoor Sabha* jumped to the loss of previously available overtime wages, bypassing the elementary concern of minimum wages.[181] Also, it is pertinent that the Supreme Court did take note of the complete proportionality between government action necessitated by circumstances and its effect on the workers.[182] In tacitly using the fifth point of the five-limbed proportionality of 'State-action' test, last re-iterated in *K.S. Puttaswamy & Anr. v. Union of India & Anr.*,[183] the

---

[178] Amartya Sen, COLLECTIVE CHOICE AND SOCIAL WELFARE 22-30 (2nd ed., 2017).
[179] *Id.*
[180] *See* discussion *infra* ¶¶ 9-10.
[181] *Gujarat Mazdoor Sabha*, *supra* note 144, ¶¶ 34-43; *See* The Factories Act, 1948, No. 63, Acts of Parliament, 1948, § 59.
[182] *Gujarat Mazdoor Sabha*, *supra* note 144, ¶¶ 10-11.6, 40.
[183] K.S. Puttaswamy & Anr. v. Union of India & Anr., 2017 10 SCC 1, ¶ 325.

Supreme Court held that the Respondent state acted disproportionately by interfering with the workers' rights without enhancing (economic) safeguards.[184] This inchoate line of reasoning misses out on proportionality in real terms, focussing only on overtime wages as the metric for 'humane working conditions'.

The loss of overtime wages ought to follow a primary consideration of loss in minimum wages, since Section 59 of the Act posits the latter to be its definitional component.[185]

As an illustration of indirect wage thefts/notional deductions, the American cases of *Arriaga v. Florida Pacific Farms*[186] and *De Luna-Guerrero v. North Carolina Grower's Association, Inc.*[187] are the most revelatory. Succinctly put, the issue before the concerned courts[188] was to determine whether the federally specified minimum wage floor was artificially breached. The employer-defendants were corporate bodies arguing that the transport costs incurred by the plaintiff-employees were neither necessary nor incidental to the work involved. The plaintiffs argued that the costs were indeed fundamental to performing the work and should statutorily be factored in while computing wage entitlements. Even though the

---

[184] *Gujarat Mazdoor Sabha*, *supra* note 144, ¶¶ 10, 42.
[185] The Factories Act, 1948, No. 63, Acts of Parliament, 1948 § 59.
[186] Arriaga v. Florida Pacific Farms L.L.C., 305 F.3d 1228 (11th Cir. 2002) (United States) ("***Arriaga***").
[187] De Luna-Guerrero v. North Carolina Grower's Association, Inc. 338 F. Supp. 2d 649 (E.D.N.C. 2004) (United States).
[188] United States Court of Appeals, Eleventh Circuit and Eastern District Court, North Carolina, respectively.

defendants paid the legal minimum wage on the face of it, they created a *de facto* deduction by denying these reimbursements. The courts in these cases determined the costs to be a necessary expense in performing official duties, and held:

"*…there is no legal difference between deducting a cost directly from the worker's wages and shifting a cost, which they could not deduct, for the employee to bear.*"[189]

The focus, therefore, is the cumulative incidence of efforts put by the employee and its proportionality with the wages. It is the very basis of International Labour Organisation's [*hereinafter* "**ILO**"] Hours of Work (Industry) Convention, 1919 (No. 1), to which India has been an original signatory. This point is made more directly by the ILO's guidelines in their formulation of non-compliance of minimum-pay rules: there needn't be direct deductions for an impermissible departure from the laws, and can be done obliquely by requiring more overtime work for the same legal minimum or skewing the 'work to pay ratio' by other means.[190]

The beneficence of the outcome in *Gujarat Mazdoor Sabha*, therefore, deserves limited credit. Demonstrably, the executive orders across state borders were bad in violating the law, regardless of the pandemic. The parts of legal reasoning where the pandemic is brought

---

[189] *Arriaga*, *supra* note 186, ¶ 1236.

[190] *Minimum Wage Policy Guide: Chapter 1: What is a Minimum Wage*, INTERNATIONAL LABOUR ORGANISATION https://www.ilo.org/global/topics/wages/minimum-wages/definition/WCMS_439066/lang--en/index.htm.

about as the primary driver for the conclusion, do not capture the intent behind the Act and minimum wages.[191]

It is proposed that the states effectively permitted underpaying minimum wages and exacerbated market coercion instead of nullifying the same. The Supreme Court in *P.U.D.R. & Ors. v. Union of India & Ors.* has laid down the precise meaning of the term 'minimum' in the context of wages to assert that there exists certain proportionality between the 'labour provided' and 'its recompense'. It then defined compulsion for Article 23, holding socio-economic compulsion to be its object, as opposed to physical force of coercion *per se*.[192] As scholar Gautam Bhatia puts it, the Indian Constitution factored in economic arrangements themselves as probable violations of rights.[193] Accordingly, it put the mandate on the government to lessen this pre-existing asymmetry between workers and employers.[194]

However, it is proposed that the Constitution went a step further than being transformative in in its formulation of Article 23. It envisaged a dynamic transfer of intra-text obligations.

---

[191] Thadeu Weber, *J. Rawls' idea of an "existential minimum"*, 54(127) KRITERION: PHILOSOPHY REVIEW 197, 200-210 (2013).
[192] *PUDR*, *supra* note 154, ¶¶ 12, 13.
[193] Gautam Bhatia, *The Transformative Constitution: A Radical Biography in Nine Acts* 191 (2019).
[194] *Id.*

D. TRANSFERENCE: A TRANSMUTATION OF SOCIO-ECONOMIC 'DIRECTIVES' TO CEMENTED 'RIGHTS'

The fundamental rights were intended to lessen the sway of non-government actors over the socio-economic lives of the citizens as well.[195] The Constituent Assembly had intended to lessen the predatory control of market forces in determining the terms of this relationship, naturally skewed toward increased work hours and reduced wages.[196] This is why the Supreme Court has previously held that minimum wage calculations ought to directly correlate with the 'specified amount of work'.[197] However, the Drafting Committee did not want to dictate economics through justiciable rights.[198] Hence, they set it out as a 'moral precept': a positive freedom for the government as opposed to a stricture.[199] This shall be a part of the signage instructing how to strive towards an ideal.[200]

It is proposed that it was as markers of a more-equalised relationship that minimal wages and 'due' economic necessity went into Part IV.[201] Extended further, it was designed to reach an eventual

---

[195] *Id*., at 205.
[196] Pramit Bhattacharya, *The economics of Ambedkar*, MINT (April 09, 2016) https://www.livemint.com/Sundayapp/lzpPlO5wsmQENPeXNWvwcK/The-economics-of-Ambedkar.html.
[197] Workmen of Bombay Port Trust v. Trustees of Port of Bombay, (1966) 2 SCR 632.
[198] SHIBANIKINKAR CHAUBE, CONSTITUENT ASSEMBLY OF INDIA: SPRINGBOARD OF REVOLUTION 170 (2nd ed. 2000).
[199] ROHIT DE, A PEOPLE'S CONSTITUTION: THE EVERYDAY LIFE OF LAW IN THE INDIAN REPUBLIC 6 (2018).
[200] Speech of Dr. B.R. Ambedkar, *Constituent Assembly Debates, Vol. VII*, (November 19, 1948), https://www.constitutionofindia.net/constitution_assembly_debates/volume/7/1948-11-19.
[201] *See infra* notes 65-67.

confluence with Part III. A dynamic link was deliberately left between Article 23(1)[202] on the one hand, and Articles 39(a) & (e),[203] 41[204] and 42[205] on the other.

To recapitulate the functioning of transference: the constitutional objective is to attain proportionality between quantum of work and the recompense it necessitates. This implies that the relevant provisions of Part IV, as and when fulfilled, will iron out the tilt in the employer-employee relationship. If these fulfilled rights are attempted to be retracted, it is akin to re-introducing the tilt. However, any government act that skews that relationship shall be hit by the equalising principle of Article 23. Hence, 'transference' works like an algebraic formulation, elevating certain fulfilled positive obligations to a heightened constitutional status.

A transference of this was illustrated when Article 39(d) was read as a part of Article 14.[206] Similarly, the jurisprudential trend since *Mukesh Advani v. State of M.P.*[207] has been to favour minimum wage as a constitutional mandate, and not merely a discretionary power under a directive.[208]

---

[202] INDIA CONST., art. 23, cl 1.
[203] INDIA CONST., art. 39, cl a, art. 39, cl. e.
[204] INDIA CONST., art. 41.
[205] INDIA CONST., art. 42.
[206] Girish Kalyan Kendra Workers Union v. Union of India, AIR 1991 SC 1173, ¶ 6; Mohini Jain v. State of Karnataka, AIR 1992 SC 1858, ¶ 7.
[207] Mukesh Advani v. State of M.P., (1985) 3 SCC 162.
[208] Atul M. Setalvad, *The Supreme Court on Human Rights and Social Justice: Changing Perspectives*, in SUPREME BUT NOT INFALLIBLE: ESSAYS IN HONOUR OF THE SUPREME COURT OF INDIA 250 (B.N. Kirpal et al. 2nd edn. 2004) ("**Setalvad**").

This was explicitly stated in *Olga Tellis & Ors. v. Bombay Municipal Corporation & Ors.*,[209] specifically for migrant workers within the country.[210] The decision went further by equating right to work[211] with another provision in Part III: the right to life.[212] It held that all powers bestowed on the government, such as those under Article 256,[213] shall be utilised to facilitate the cementing of this right.[214] The Supreme Court further explicated the same assertion in *All India Imam Organization v. Union of India*.[215] Therein, it was held that the perceived financial difficulties of an institution cannot possibly form a basis for determining applicability of the fundamental rights of a citizen.[216] The decision in the case was strictly limited to payment of minimum wages, and not its proportionality with work. However, the notable feature of it was that it equated a directive principle to a fundamental right.[217]

This transference of obligation from Part IV to Part III was most uniquely summarised in *D.T.C. v. D.T.C. Mazdoor Congress*.[218] The power relations between an employer and employee will always be tilted towards the former, it stated.[219] The Supreme Court ingenuously stated that

---

[209] Olga Tellis & Ors. v. Bombay Municipal Corporation & Ors., (1985) 3 SCC 545 ("***Olga Tellis***").
[210] *Id.*, ¶¶ 32, 33.
[211] INDIA CONST., art. 41.
[212] INDIA CONST., art. 21.
[213] INDIA CONST., art. 256.
[214] *Olga Tellis*, *supra* note 209, ¶¶ 32, 33.
[215] All India Imam Organization v. Union of India, (1993) 3 SCC 584.
[216] *Id.*, ¶ 6.
[217] Minerva Mills Ltd. v. Union of India, (1980) 3 SCC 625, ¶ 105 ("***Minerva Mills***").
[218] D.T.C. v. D.T.C. Mazdoor Congress, (1991) Supp(1) SCC 600 ("***DTC***").
[219] *Id.*, ¶ 232.

adequacy of payments, in light of the performative nature of the work involved, becomes crucial for the right to livelihood.[220] Income becomes a foundation for many fundamental rights.[221] This necessarily implies adequacy of payment as a constitutional guarantee falling under Part III. The said obligation includes conceiving a levelling mechanism in employment relationships.[222]

In another instance, 'job security' in its widest sense was held to comprise of concretely anchored living wages, to secure a fundamental right.[223] This sought-for transference was held as indispensable even during the most exigent of financial circumstances.[224]

This reasoning delegitimises the underlying ground for Section 5 notifications, which was the financial stress induced by an unforeseen exigency. Even assuming this to be a valid argument, the prevailing law preemptively rebuts it.[225] It contrarily suggests that work of greater utility and value under difficult circumstances, necessitating minimum wages *a fortiori*.[226] In line with this, precedent further bars a negative revision of minimum wages on account of the financial stringency of the institution as a whole.[227]

---

[220] *Id.*
[221] *Id.*
[222] Consumer Education & Research Centre v. Union of India, (1995) 3 SCC 42, ¶¶ 24, 25.
[223] Sanjit Roy v. State of Rajasthan, (1983) 1 SCC 525, ¶ 3 ("**Sanjit Roy**").
[224] *Id.*, ¶ 4.
[225] *Id.*
[226] *Id.*; *see also* State of Gujarat v. Hon'ble High Court of Gujarat, (1998) 7 SCC 392.
[227] The Workmen represented by Secretary v. The Management of Reptakos Brett and Co. Ltd., (1992) 1 SCC 290, ¶ 28 ("***Reptakos Brett***").

Demonstrably, the jurisprudence has consistently held the obligation on minimum wages is subject to 'transference'. That is, the minimum-wage requirement may have its roots in Part IV, but that is only a baseline allocation. Proposedly, once the State initiates beneficial legislation/positive action based on the obligations in this Part of the Constitution, those become cemented bases for future actions. The benefits granted in the said direction can only be built upon, and not negated in any manner. It is submitted that the implications of the said beneficial legislations/positive actions by the State acting under Part IV become cemented 'rights'. Applying the said proposition, previously granted minimum wages for a certain period of work hours are proposed to be protected by the negative rights as against the State. Once guaranteed in any form, their retraction will have to be tested against Article 23. At the very least, the Constitution requires that minimum wages be given the most expansive interpretation, eventually moving towards living wages as the bare minimum.[228]

It is submitted that the obligation of minimum wages is also covered by transference of a different kind: directive principles to the basic structure. This is asserted as is because, *inter alia*, the strictures ensuring efficiency in work are considered to be the essence of the 'right to work' as espoused by Article 39(a).[229] More specifically in the context of minimum wages, this right and all its subsets were considered to be the very essence

[228] Express Newspapers v. Union of India, AIR 1958 SC 578.
[229] Daily Rated Casual Labour v. Union of India (1988) 1 SCC 122 at 123-124.

of the Preambular 'socialism'.[230] Striving towards socialism by enacting a comprehensive labour law framework,[231] in turn, was held to be a part of the Constitution's basic structure.[232] Hence, the proportionality between working hours and minimum wages is an extension of a very elementary feature of the Constitution. Furthermore, the basic structure view is more applicable for directive principles that have multi-provisional implications: they may function like a figurative 'cheque' to be cashed, if they have the effect of furthering the objective of a fundamental right.[233]

Logically extended, upon fulfilment and integration with a fundamental right, all the instruments wielding that effect are effectively on a figurative solid ground. Thereupon and thereafter only, further construction is permitted. The reasoning espoused by this Section is only buttressed by the fact that the amendatory Factories Act and the Minimum Wages Act, 1948 were passed by the Constituent Assembly itself, following a year of discussions on the draft of Article 23.[234] The fulfilled positive obligation of 'minimum wage-rate' comes to acquire elevated constitutional

---

[230] *Reptakos Brett*, *supra* note 227.

[231] National Engineering Industries Ltd. v. Shri Kishan Bhageria, (1988) Supp SCC 82 ¶ 14, ("***Bhageria***").

[232] Samatha v. State of Andhra Pradesh, (1997) 8 *SCC* 191, ¶¶ 79, 99; *see also Minerva Mills*, *supra* note 217, ¶ 112.

[233] SUDHIR KRISHNASWAMY, DEMOCRACY AND CONSTITUTIONALISM IN INDIA: A STUDY OF THE BASIC STRUCTURE DOCTRINE 39, 40, 82, 179 (2009).

[234] *Discussion on Clause 11-Traffic in Human Beings*, CONSTITUENT ASSEMBLY DEBATES, VOL. III, (May 01, 1947), https://www.constitutionofindia.net/constitution_assembly_debates/volume/3/1947-05-01; Government of India Act, 1935, First Schedule, § 18; Raghu Vinayak Sinha et al., *A brief legal history of the Minimum Wages Act (1948) and its implementation in India*, 33 SADF FOCUS 1, 1-3 (2017).

sanctity. The only powers of the states under Section 5 of the Act should be to enhance the law, not negate it.

III. 'RETROGRESSION' FROM A CONSTITUTIONALLY DESIRED POSITION IS IMPERMISSIBLE

There seems to be another feature that becomes salient in case such as this. By fixing minimum wage rates and working hours, a society freezes its achieved progress in the form of legislation. This progressive element alone, apart from the joint textual aims of the preamble, directive principles and fundamental rights, is a law unto itself. The mere phraseology of Article 23 *per se* carries a connotation of 'irreversibility' in secured human rights for the workers.

A. THE SKELETAL FRAMEWORK: ORIGINS OF THE NON-RETROGRESSION PRINCIPLE

Before the amending notifications, the workers enjoyed a guarantee in form of a floor-limit on working hours, both within a day as well as a week, along with a shorter cumulative spread-over per day. However, when the states bring about a substantial change in these, there occurs a dilution of rights *per se*. This is regardless of the *de facto* deductions or the nuanced application of the basic structure doctrine, as discussed previously. This Section argues the emerging constitutional principle of non-retrogression bars the states from bringing about even a slight detriment in the existing rights-based framework.

The roots of this principle may be traced back to an interesting feature in the Universal Declaration of Human Rights [*hereinafter*

"**UDHR**"],[235] a declaration contributed to by India. It attempted to cement the progressive realisation of human rights achieved by way of legislation in a democratic setup.[236] In its Article 30,[237] the UDHR states that no government should act in a way to destroy the rights set as its purposive ideal. Article 2(1)[238] of the International Covenant on Economic, Social and Cultural Rights [*hereinafter* "**ICESCR**"] is similarly phrased.[239] These, hence, not only act as sources of substantive social rights, but also espouse a unidirectional growth thereof.[240] The underlying premise is that once the rights are created or augmented by progressive legislation or interpretation, a government cannot retrograde to a position that was less advantageous to its constituents. The flow of changes to the rights-based framework has to be strictly unidirectional, complementing the pre-existing enjoyment of rights.

---

[235] G.A. Res 217 (III) A, The Universal Declaration of Human Rights (December 10, 1948), art. 30; Miloon Kothari, *Remembering India's Contributions to the Universal Declaration of Human Rights*, THE WIRE (December 20, 2018), https://thewire.in/rights/indias-important-contributions-to-the-universal-declaration-of-human-rights ("**Kothari**").

[236] Katherine Young, *Waiting for Rights: Progressive Realization and Lost Time*, BOSTON COLLEGE LAW SCHOOL FACULTY PAPERS 1, 6-12 (2019) ("**Young**").

[237] G.A. Res 217 (III) A, The Universal Declaration of Human Rights (December 10, 1948), art. 30.

[238] G.A. Res 2200 (XXI), The International Covenant on Civil and Political Rights (March 23, 1976), art. 2.

[239] Young, *supra* note 236, at 8-10.

[240] Laura Kirvesniemi, *Prohibition of Retrogression: Effectiveness of Social Rights in the Finnish System of Constitutional Review* 19-33 (August, 2015) (Unpublished M. A. thesis, University of Helsinki), https://helda.helsinki.fi/bitstream/handle/10138/157497/Master's%20thesis%20Laura%20Kirvesniemi%20final.pdf?sequence=2 (March 29, 2021); UN, *Principles and Guidelines for a Human Rights Approach to Poverty Reduction Strategies*, ¶ 4, HR/PUB/06/12 (June, 2006).

Regardless of an economic crisis, a cut-back in expenditure that takes away an 'existential minimal' amounts to being constitutionally regressive.[241] When Indian states reduce working hours under a law enacted by the Parliament, they retrograde to a lesser beneficial position for the workers. That is, a position where a fundamental right's implementation was in the form of a less enabling entitlement.

B. FLESHED UP WITH CONSTITUTIONAL COLOUR: THE CONCEPT'S DEVELOPMENT IN THE UNITED STATES

To understand the concept of non-retrogression in guaranteed rights, a backdrop of the concept's judicial usage is necessary. It was devised as a constitutional exception to the 'reserved power of states' in the United States of America's [*hereinafter* "**U.S.**"] federal set-up.[242] For a change, the supposedly weaker U.S. federal government may trump state law(s) for a particular subject if it legislates more beneficially towards human rights.[243] From thereon, that law may only be overwhelmed if a better state legislation comes along. Any extraneous crises that may occur shall only make any such legal dilutions even more directly assailable by this principle.[244] The authorities, as will be demonstrated below, suggest that the beneficial law may have come about any under any local/central constitutional power;

---

[241] Matheus Medeiros Maiaa & Rafael Soares Duarte, *Analysis of the (Im)Possibility of Social Retrogression in the Brazilian Constitutional Order*, 5(11) SOCIOLOGY STUDY 875, 876-882 (2015).
[242] John C. Jeffries & Daryl J. Levinson, *The Non-Retrogression Principle in Constitutional Law*, 86(6) CALI. L. REV. 1211, 1214 (1998) ("**Jeffries**").
[243] *Id.*, at 1234.
[244] Robert S. Berman, *Constitutional Law: Due Process: Non-Retrogressive Reapportionment Plan Upheld (Beer v. United States)*, 60(1) MARQUETTE L. REV. 173, 180, 183 (1976).

however, its retraction/dilution can always be tested for retrogressing from U.S. constitutional objective.

Although never explicitly linked with the UDHR, the principle is claimed to be first founded by the U.S. decision in *Reitman v. Mulkey* [*hereinafter* "***Reitman***"].[245] Like most of its successor decisions[246] which fleshed the concept up, the case dealt with an amendment to the California Constitution which did away with beneficial legislation. The issue was whether the state of California was well within its rights to amend the state Constitution in a manner that skewed the progress achieved as per U.S. Constitution's Fourteenth Amendment [*hereinafter* "**equality clause**"]. The Supreme Court of the United States [*hereinafter* "**SCOTUS**"] concluded that the U.S. Constitution cannot be said to govern the aspect of the Californian Constitution which affects housing.[247] However, and at the same time, it isn't permissible for the state to deteriorate a better law that had the effect of restricting horizontal discrimination in housing policies.[248] The legal reasoning for the conclusion was this: the political power (as a consequence of the laws) previously granted to a certain group of (marginalised) citizens constitutes only a baseline allocation.[249] The impermissible direction of

---

[245] Reitman v. Mulkey, 387 U.S. 369 (1967) (United States) ("**Reitman**").
[246] Shaw v. Reno, 509 U.S. 630 (1993) (United States); Holder v. Hall, 512 U.S. 874 (1994) (United States); Miller v. Johnson, 515 U.S. 900 (1995) (United States).
[247] *Reitman*, *supra* note 245, at 388.
[248] *Id.*, at 373-381.
[249] *Id.*, at 394.

change would be when a subtraction from this allocation takes place, by an act of the executive or the legislature.[250]

The principle was re-affirmed by the SCOTUS in *Hunter v. Erickson*.[251] The issue here was whether a city of a state can amend its city charter to achieve the same effect as in *Reitman*. As in *Reitman*, the issue here was whether the equality clause of the Fourteenth Amendment to the U.S. Constitution applied to the given case. Again, the U.S. Constitution's clause was read as prohibiting an act that retrogrades from (such) a right enhancing law for being *per se* discriminatory.[252] To pre-empt this retrogression, the equality clause is not barred by any reserved legislative/executive powers that a state may otherwise have.[253] The decision's major premise posited that any tinkering of beneficial law, meant for those on the social margins, would be retrograde.[254]

The most pertinent enunciation for an expansive scope in its application came in *South Carolina v. Katzenbach*.[255] The issue here was again whether the SCOTUS can apply the equality code so as to govern a decision made by the state, ostensibly under its domain of reserved powers. Herein, the issue was stringent voting eligibility criteria for states with a certain voter turnout. One of the states refused to comply with this federal imposition,

---

[250] *Id.*
[251] Hunter v. Erickson 393 U.S. 385 (United States).
[252] *Id.*, at 397.
[253] *Id.*
[254] Washington v. Seattle School District No. 1, 458 U.S. 457 (1982) (United States) ("**Seattle School District**").
[255] South Carolina v. Katzenbach, 383 U.S. 301 (1966) (United States).

and this act of protest was upheld by the SCOTUS. The SCOTUS explained that the object of the concept is, to tilt the weight of time and inertia in favour of the socially weaker class, by freezing the pre-existing beneficial framework.[256] It is this reasoning that applies to minimum wage workers with previously fewer working hours.

It is also pertinent to mention that in addition to the cases cited above, there exists an instance in *Denver Area Educational Telecommunications Consortium v. F.C.C.*[257] wherein a morphed application of the principle takes place. Herein, a statute enacted by the federal government for reserving some part of private broadcasting space for federal use was under challenge by cable operators.[258] The relevant laws involved were the First Amendment of the U.S. Constitution [*hereinafter* "**freedom of expression clause**"], along with limits on the power of the federal government under Article 1, Section 8, Clause 3 (*i.e.*, the commerce clause) and Cable Television Consumer Protection and Competition Act, 1992. The SCOTUS, initially, stated that such a provision had the effect of restricting the freedom (of expression) available to private cable operators.[259] This was seen as a retrogression from the private operators' freedom to express, as encapsulated in their power to editorialise.[260] This was taken more in consonance with fulfilling the freedom of expression clause. However,

---

[256] *Id.*, at 328.
[257] Denver Area Educational Telecommunications Consortium v. F.C.C., 518 U.S. 727 (1996) (United States).
[258] *Id.*, at 770.
[259] *Id.*
[260] *Id.*, at 761, 773.

because the concerned statute was historically preceded by federal frameworks which never bestowed full autonomy on the operators, the SCOTUS stated that there was no retrogression.[261] The principle would only apply if the previously available position was deviated from. Hence, in this case, the Court did judge the impact of the statute on larger constitutional objectives, but on a chronological comparison of the constitutional subjects' statuses.[262] This case, therefore, disregards the fulfilment of constitutional objectives and only looked at the existence of any 'demotion in circumstances'.

The principle, taken from a strict constitutional effect perspective, or even from a chronological comparison of the subject's status point of view, applies squarely to the case at hand in nullifying the 2020 notifications. In the case of Section 5 of the Act, a state government may legally be permitted to bring about changes in the law. However, the same would be deemed ineffective because of it diminishing an enhanced rights-based position envisaged by the Constitution. That is, the notifications are retrogressing to a position where the class with lesser or no means becomes more susceptible for higher labour-value extraction. Alternatively, the prior proportionality between working hours and minimum wages bars a retrogression from the same. This is not accompanied by any proportional increment in the employer's obligations, and hence, is a demotion in

[261] *Id.*, at 760-761.
[262] Jeffries, *supra* note 242, at 1232.

circumstances. Non-retrogression bars such a retreat to what is otherwise permissible, but a less desirable, position.[263]

C. IMPORT TO INDIA AND ITS PROBABLE DEFEASANCE OF THE 2020 NOTIFICATIONS

In India, the tacit embodiment of this principle has been in existence. Cases dealing with standards in labour law dictate that the government may only expand them, 'legislation to legislation'.[264] The same is aligned with cases that espouse the disparate impact test. The concept was created by the U.S. for its labour law jurisprudence,[265] and accepted by India in its larger scheme of non-discriminatory provisions.[266] Essentially, it argues that any change in legal circumstances may not perceivably violate the Constitution.[267] However, given the vulnerabilities of certain sections in the society, a violation may occur in their covert yet inferior treatment.[268] It may be asserted that in a figurative sense, the non-retrogression principle acts as a broader version of this concept. While it discerns and strikes down any retrogression in circumstances, the disparate impact has to check its

---

263 *Seattle School District*, *supra* note 254, at 485.
264 *Bhageria*, *supra* note 231, ¶ 14.
265 Michael Selmi, *Was the disparate impact theory a mistake?*, 53(3) UCLA L. REV. 701, 708-714 (2006).
266 Dhruva Gandhi, *Locating Indirect Discrimination in India: A Case for Rigorous Review under Article 14*, 13(4) NUJS L. REV. 1, 4 (2020); Shreyas A.R., *On the Dangers of Reading Disparate Impact into Manifest Arbitrariness – a Response to Dhruva Gandhi*, INDIAN CONSTITUTIONAL LAW AND PHILOSOPHY (September 12, 2020), https://indconlawphil.wordpress.com/2020/09/12/guest-post-on-the-dangers-of-reading-disparate-impact-into-manifest-arbitrariness-a-response-to-dhruva-gandhi/.
267 Tarunabh Khaitan, *Indirect Discrimination* 4 (Melbourne Legal Studies Research Paper Series No. 854, 2017).
268 *Id.*

impact on specific groups. It is submitted that the non-retrogression principle is recognised insofar as it overlaps with the latter.

During the Constitution Assembly Debates, interestingly, an amorphous proto-version of this constitutional concept was cited. In arguing against the uniformity of laws in certain subjects, A. Thanu Pillai interposed that some states had made more progress in the human rights framework than others and possibly the nascent Centre.[269] If an imposition of the latter's framework takes place over the former, it shall lead to an unjust 'retrogression'.[270] Put succinctly, he was suggesting that the new Constitution let all legislatures compete for better human rights laws, freezing the better ones as unassailable standards.

However, there exists no wholesale adoption of the principle by the Indian Constitution. Notably, India is a signatory to both UDHR and the International Covenant on Economic, Social and Cultural Rights (ICESCR).[271] Fortuitously, the arc of constitutional jurisprudence does reveal a willingness and a probable adoption of the argument made by Pillai. Most illustratively, the Supreme Court in *Bandhua Mukti Morcha v. Union of India & Ors.*[272] conceptualised a dynamic concretisation of right-enhancing

---

[269] Speech of Shri A. Thanu Pillai, *Constituent Assembly Debates, Vol. XI*, (November 24, 1949), https://www.constitutionofindia.net/constitution_assembly_debates/volume/11/1949-11-24.

[270] *Id.*

[271] Treaty Section, United Nations, *United Nations Treaty Collection: Chapter IV*, https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-3&chapter=4&clang=_en; *See* Kothari, *supra* note 235.

[272] Bandhua Mukti Morcha v. Union of India & Ors., (1984) 3 SCC 161 ("**Bandhua Mukti Morcha**").

laws. It states that a constitutional violation may occur simply due to the non-implementation of laws that secure the dignity of workmen.[273] The reason proffered by the Supreme Court for this assertion was retrogression and the resultant nullification of constitutional intent:

"…*they would become more exposed to exploitation and slide back once again into serfdom even in the absence of any coercion.*"[274] [emphasis supplied]

The judgement is denoting that anything apart from a progressive interpretation and implementation of laws shall be defeating a rights-based objective.[275] It logically follows that a serious attempt at giving pre-existing labour standards a dynamic and irrevocable constitutional salience.

The only explicit recognition of the principle occurred in *Navtej Singh Johar & Ors. v. Union of India*.[276] In stating that progressive realisation of rights has non-retrogression as its corollary, a government cannot retrograde to a position that conduces a lesser enjoyment of the same rights. The government has indeed covered some distance forward down the road to fulfilling a directive principle in cementing a minimal for working hours.[277] The principle also prevents the State from decelerating its pace at

---

[273] *Id.*, ¶ 26; P.P. Rao, *The Supreme Court and the Employee*, in SUPREME BUT NOT INFALLIBLE: ESSAYS IN HONOUR OF THE SUPREME COURT OF INDIA 385 (B.N. Kirpal et al. 2nd ed. 2004).

[274] *Bandhua Mukti Morcha*, *supra* note 272, at 208.

[275] Setalvad, *supra* note 208, at 251.

[276] Navtej Singh Johar & Ors. V. Union of India, (2018) 10 SCC 1.

[277] *See* Paul Wolfson, *A review of the consequences of the Indian minimum wage on Indian wages and employment*, Working Paper ILO ASIA- PACIFIC WORKING PAPER SERIES, 7-10, 14 (May, 2019), http://oit.org/wcmsp5/groups/public/---asia/---ro-bangkok/---sro-new_delhi/documents/publication/wcms_717971.pdf.

which it proceeds towards this constitutional goal. The Supreme Court has also stated that an act that consolidates the rights under Part III and furthers the directive principles adheres to the "*foundational Constitutional principle of non-retrogression*".[278] Invoking the Act to mutilate an achieved threshold such as the one discussed above, is nothing but constitutionally regressive in the Indian context.

IV. CONCURRENCE IN DELIBERATIVE POWERS HAS ITS LIMITS APART FROM REPUGNANCY

Legal scholar H.M. Seervai had fleetingly mentioned a novel ground for repugnancy in the context of concurrent list subjects: in case a state amendment makes the application of certain provisions of the central act effectively harsher relative to similarly situated citizens in other states, it shall be violating Article 14.[279] Even without the equality aspect, this formulation raises a larger argument. A state cannot fiddle with the Union's legislative framework, arbitrarily, against the interest of its residents.

The Indian Constitution's source of federal-concurrent legislative jurisdiction happens to be its Australian counterpart.[280] In case of an inconsistency, both the jurisdictions prioritise the Central law on the subject.[281] However, the Australian jurisprudence surrounding concurrent list disputes had devised two tests for discerning the existence of this

---

[278] *Id*., at 125, 146.
[279] H.M. SEERVAI, CONSTITUTIONAL LAW OF INDIA: A CRITICAL COMMENTARY 468 (4th ed., 2004).
[280] INDIAN LAW INSTITUTE, CONSTITUTIONAL DEVELOPMENTS SINCE INDEPENDENCE 217 (1975).
[281] 1 M.P. Jain, INDIAN CONSTITUTIONAL LAW, 94 (6th ed 2011).

inconsistency. These happen to be: i) 'cover the field' test; and ii) 'interference or denial of rights' test. Both have their source in the Australian Constitution's Section 109, which is the equivalent of Article 254(1) of the Indian Constitution.

In essence, the 'cover the field' test deals with a quantitative analysis of comparing the Union and provincial frameworks regarding a legislative subject. The federal unit that appears to be more meticulous in governing the legislative field shall prevail, nullifying minor amendments by the other. This has witnessed wide acceptance in the Indian jurisprudence. Whereas, the 'interference or denial of rights' test has not acquired similar currency. According to this second test, concurrent jurisdiction gets disabled as and when it's attempted for wresting away an existing right. There need not exist a repugnancy *stricto sensu*. The bar is on the otherwise imperceptible implication of some concurrent laws: nullifying each other's right-based benefits.

The following sub-sections argue against the impugned notifications, both equally invalidating the same. The Act, as an act of Parliament of India, came with desirable stipulations for working hours, only enabling the states to enhance them. Similarly, both the Centre and the states may have the power to direct minimum wages, but it is the former that carries more weight.

A. THE 'EXHAUSTIVE FIELD' TEST DECLARES THE UNALTERED UNION LAWS AS STARTING LINES

Succinctly put, this concept shall reveal how the Indian Union has exclusively appropriated deliberation in working conditions and minimum wages for itself.[282] However, the argument for its application herein shall have to be prefaced with its historical roots in Australian labour law.

i. The Concept's Natural Congruity with Labour Rights

The foundation, notably, is situated in the Australian minimum-wage jurisprudence. In the relevant period, Australia had a federal law[283] for addressing labour law disputes, which has been a concurrent subject under the Australian Constitution.[284] Such disputes had to be compulsorily resolved by a vestigial organ of the Central government.[285] It settles the case by way of an 'arbitral award'.[286]

Notably, the zone of concurrence in this subject was deemed hazy in a series of cases before the High Court of Australia [*hereinafter* "**the High Court**"]. It began when it came across a case titled *Australian Boot Trade Employees' Federation v. Whybrow & Co.*[287]

---

[282] *See* discussion *infra* at 20-22.
[283] Commonwealth Conciliation and Arbitration Act, 1904 (Australia) (repealed 1989).
[284] Ron McCallum, *The Australian Constitution and the Shaping of Our Federal and State Labour Laws*, 10(2) (2005) DEAKIN L. REV. 460 (2005) ("**McCallum**").
[285] *Id.*
[286] *Id.*
[287] *Australian Boot Trade Employees' Federation v. Whybrow & Co.* (1), (1910) 10 CLR 266 (Austl.) ("***Whybrow***").

Therein, the primary issue was whether such an award stipulating a higher minimum wage-floor would trump the lower state floor-limit. In other words, this would be encroaching the reserved powers of the states, the exact opposite of the Indian position.[288] The High Court chose to shape a pre-existing amorphous concept, namely, the 'simultaneous-obedience' prism.[289] It stated that adherence to the Central law on minimum wages would necessarily entail default compliance with the lower minimum stipulated by the states. Applying this, it concluded the Central condition to be supplementary and not inconsistent.[290] However, this approach kept the state level floor limit alive. Isaacs J., in a separate concurring opinion stated that the higher floor limit set-up by the majority should now be the new law for the state. He adumbrated what later became the 'cover the field' test, by analysing the award as a federal law contradicting state legislation.[291] According to his reasoning, the federal law intended to govern the specifics of labour law disputes. This intent could supposedly be revealed by, either: the greater number of laws or a much-enhanced interpretation of the same law.[292] In this case, by comparing the specificity in legal frameworks at both federal levels, he concluded that it was largely the Centre's intention to minimise labour disputes.[293] A higher minimum in wages implied fewer

---

[288] M.P. JAIN, INDIAN CONSTITUTIONAL LAW 821 (Jasti Chelameswar J. & Dama Seshadri Naidu J. eds., 8th ed., 2018).
[289] *Whybrow*, *supra* note 287, at 299.
[290] *Id.* at 330.
[291] McCallum, *supra* note 284.
[292] *Whybrow*, *supra* note 287, at 310-312.
[293] *Id.*, at 332.

labour disputes, and hence, the federal floor limit was deemed a better approximate to the federal intention.[294]

He had first thought of it in *Clyde Engineering Co. Ltd. v. Cowburn* [*hereinafter* "***Cowburn***"],[295] another case dealing with minimum wages. Stated more clearly, it held this intention could be evinced by greater number of laws by either of the vertical-federal units. Once this quantitative edge is established, the other unit may only exercise its concurrent power so as to enhance the other's intent. Another case stated that such an award in minimum wages evinces explicit intention to completely expropriate the state's concurrent power.[296] This view doesn't seem to have found any purchase in the Australian jurisprudence.

Isaac J's view, albeit approved in obiter instances otherwise,[297] was truly consolidated in *Blackley v. Devondale Cream (Vic) Pty. Ltd.*[298] The High Court held that Section 109 of the Australian Constitution found direct application in such a case.[299] It stated that this wasn't about simultaneous obedience of supplementary laws, but about a collision of standards on wage-minimums.[300] Upon a purely quantitative analysis of legal provisions,

---

[294] *Id.*
[295] Clyde Engineering Co. Ltd. v. Cowburn, (1926) 37 CLR 466 (Austl.) ("***Cowburn***").
[296] Woodstock Central Dairy Co. Ltd. v. Commonwealth, (1912) 15 CLR 241 (High Court of Australia).
[297] *Cowburn*, *supra* note 295.
[298] Blackley v. Devondale Cream (Vic) Pty. Ltd., (1968) 117 CLR 253 (High Court of Australia) ("***Blackley***").
[299] *Id.*, at 259-263.
[300] *Id.*, at 258-259.

the federal law seemed to impose a greater obligation on the employer, which is in line with the larger object of labour law.[301]

The High Court in *Ex parte McLean*[302] finally went to consolidate the higher floor rate of its own choosing across the states, and not just to those present as parties. It stated that state laws may continue to exist. But if the Centre chooses to become more comprehensive or specific in a certain aspect of that legislative field, it acquires a dominant status for that aspect.[303] In other words, a legislative field such as 'working conditions' implies many elementary areas: gratuity payments, minimum wages, working hours, etc. Both states and the Centre may legislate concurrently, but exclusivity to govern each shall depend on the comprehensiveness of laws for each.

Succinctly put, this is how the test seems to operate: a comparative view of both the central and state-level legal frameworks takes place. The one with the quantitatively superior framework is perceived to govern a certain area within the marked legislative field, or the whole of it. The other unit, then, may only utilise concurrent powers in enhancing the former's stipulations in this area/field, and not negating it.

---

[301] *Id.*, at 259.
[302] Ex parte McLean, (1930) 43 CLR 472 (High Court of Australia) ("***McLean***").
[303] *Id.*, at 483.

ii. Application to the Indian Concurrent Scheme of Labour Law

It is submitted that this principle has its basis in the same logical arc as espoused by Seervai. This is insofar it seems to hold a Union law as the prevalent one, in spite of being competently contradicted by a state. The more extensive a federal unit's legal framework on the subject, the more beneficial for the state's residents. Indian Union presently sees 41 labour laws enacted by it,[304] with both the laws on Minimum Wages Act, 1948, with the Industrial Disputes Act, 1947 and the Factories Act, 1948 delegating only minimal amendatory powers to states.[305] In this context, it appears that the Union has exhibited greater intent to govern disputes related to minimum wages and working conditions.[306]

Hence, if the exhaustive field test is applied, it is bound to hold the Union law's specified minimum as the prevailing one. India has explicitly adopted the test from the Australian jurisprudence. It has found widespread application under Article 254(1) of the Constitution.[307] So much so that the

---

[304] Ministy of Labour and Employment, Government of India, *List of Central Labour Laws Under Ministry of Labour and Employment*, https://labour.gov.in/sites/default/files/Central%20Labour%20Acts.pdf.

[305] P.B. Mukharji, *Delegated Legislation*, 1(4) JOURNAL OF THE INDIAN LAW INSTITUTE 465, 470-473, 476-477; State of Assam v. Horizon Union, (1967) 1 SCR 484 ("***Horizon Union***").

[306] *See also* Bloomberg, *India's heavy-handed labour laws are a result of states being a little too united*, FINANCIAL EXPRESS (June 11, 2020), https://www.financialexpress.com/economy/indias-heavy-handed-labour-laws-are-a-result-of-states-being-a-little-too-united/1988243/.

[307] Vijay Kumar Sharma v. State of Karnataka, (1990) 2 SCC 562 ("***Vijay Kumar Sharma***"); Ravula Subba Rao v. C.I.T., (1956) SCR 577; M. Karunanidhi v. Union of India, (1979) 3 SCC 431; State of Uttarakhand v. Kumaon Stone Crusher (2018) 14 SCC

Supreme Court has extended it to even Article 246, which means it is not confined to List III disputes exclusively.[308] To apply this, the Supreme Court unequivocally states that an intention to dominate a deliberative field may take any form.[309]

There may be possible objections to applying exhaustive field test in the factual circumstances of the 2020 notifications. *Firstly*, the Parliament expressly delegated powers to the state executive for modifying the relevant provisions of the Act.[310] *Secondly*, the Parliament has assigned the task of setting up wage floors to the states under the Minimum Wages Act.[311] Alternatively or cumulatively, it may be argued that the intention was not to govern this field exclusively.

However, the very basic premise of this test is that the intention applies to a certain aspect of the concurrent subject.[312] In this case, that would be the aspect of work hours, or the work-hour to minimum-wage ratio. Furthermore, a framework need not be exhaustive *strictu sensu*. According to a Constitutional Bench ruling, it only needs to be relatively

537; Offshore Holdings (P) Ltd v. Bangalore Development Authority, (2011) 3 SCC 139; Bharat Ram Gupta v. State of Uttar Pradesh, (1978) SCC OnLine All 888 (Allahabad High Court, India); G.P. Stewart, Collector of Sylhet v. Brojendra Kishore Roy Choudhury, (1939) SCC OnLine Cal 116 (India); Shabeer Shajahan v. State of Kerala & Ors., (2020) SCC OnLine Ker 2315 (Kerala High Court, India).

[308] State of Kerala v. Mar Appraem Kuri Co. Ltd., 2012 7 SCC 106 ("***Mar Appraem Kuri***"); I.T.C. Ltd. v. State of Karnataka, 1985 Supp SCC 476.

[309] Ch. Tika Ramji v. State of U.P., 1956 SCR 393, ¶¶ 28-30.

[310] *See* Factories Act, 1948, No. 63, Acts of Parliament, 1948, §§ 2(cb)(ii), 5, 84.

[311] *See* Minimum Wages Act, No. 11, Acts of Parliament, 1948, 1948, §§ 2(b)(ii), 3.

[312] *Cowburn*, *supra* note 295, at 490, 505; *McLean*, *supra* note 302.

more so than the state-level legal lattice.[313] Furthermore, in applying this test, the Supreme Court seems to have recognised that Parliamentary intent to govern labour law may have exceptions, and the same does not negate the otherwise implied intention to dominate.[314]

Hence, the express delegation of powers to modify certain provisions of the Act is no bar to the application of the test. This is explicitly demonstrated by the decision in *State of Assam v. Horizon Union*.[315] The concerned Central law (*i.e.*, Industrial Disputes Act)[316] both pre-existing and its amended version around the time, contemplated state appointment of members for the tribunals. The bar was the admittance of district court judges with a certain amount of experience. The state amendment subverted this requirement in an amendment to the Central law. The express intention of the delegation of this power in the Central law was held not to overshadow the exhaustiveness of the code.[317] The state was held to be empowered in only adding to the baseline given by the Central law, not in negating it. For the enterprise of this paper, there occur two baselines: ceiling on working hours and a (proportional) floor of minimum wages.

It is submitted that the notifications in question may only stand when these nationally specified baselines are not breached. A cap on working hours in the unaltered Central law is only a starting point and that

---

313 *Mar Appraem Kuri*, *supra* note 308, ¶ 57.
314 *Vijay Kumar Sharma*, *supra* note 307, ¶¶ 69, 70, 75, 88.
315 *Horizon Union*, *supra* note 305.
316 *See* INDIA CONST., Schedule VII, List III, *Concurrent List*.
317 *Horizon Union*, *supra* note 305.

states, through Section 5, may only lower them. Similarly, the prevailing minimum wage figures notified[318] by the Centre may only be improved upon.

B. THE 'DENIAL OF RIGHTS' TEST DISABLES THE STATES' RETRACTIVE POWERS

It is to be noted that in *Cowburn*,[319] the same court came up with a non-retrogression variant of the 'exhaustive-field test'. The 'enhanced interpretation' prong was infused with another meaning. Before exploring the same, the case deserves a greater introduction.

i. The Eerily Similar Circumstances for which the Test was Devised

The case had striking similarities with the factual circumstances of this paper's enterprise. The federal dispute resolution body, therein, gave an award mandating minimum wages for a workweek of 48 hours. The State of New South Wales, by way of legislation, targeted this award by modifying the floor to 44 hours. The latter may appear more beneficial at the surface for a moment, however, the State law was attempting to ingratiate the employers through this move. Overtime pay was still available only when the previous limit of 48 hours was crossed by the employees. A part of the Bench had applied the exhaustive-field test to invalidate the state law.[320]

---

[318] Ministry of Labour & Employment, Minimum Wages order dated 06.10.2017, No. 1/13(1)/20 17-LS-II (Notified on September 06, 2017) https://clc.gov.in/clc/node/568.
[319] *Cowburn*, *supra* note 295.
[320] *Id.*, at 472, 489-491.

The other part devised the 'interference with rights' or 'the denial of rights' test.

It posits that when a vertically-federal unit takes away or diminishes a statutorily conferred entitlement, it will be held as an invalid exercise of the concurrent jurisdiction.[321] In this case, the otherwise minimum wage entitlement was nullified if the employee worked a minute less than 48 hours. This would 'alter, detract or impair'[322] the beneficial effect of Central law for those working for 44 hours, and was invalid *ab initio*.[323]

The Court, therefore, struck at the very heart of an asymmetrical wage to hour ratio using this logic. In doing so, it also pointed out the flaw in applying the exhaustive field test in the specific circumstances of that case. Hence, this test is consequentialist insofar as it looks at government actions on a case by case basis. Complementary units in a federation shall only add, and not denature, the rights given by each.

Pertinently, a similar yet incomplete argument was indeed raised before the Supreme Court in *Gujarat Mazdoor Sabha*, but in the context of lost overtime-wages. Section 59 doubles the ordinary wages for work-hours exceeding the statutory cap.[324] By pushing the cap further upwards, there occurs an artificial theft in overtime wages, much like the *de facto* deduction in minimum wages discussed in the beginning.[325] The Supreme Court in its

---

[321] *Id.*, at 478, 479, 502.
[322] Victoria v. Commonwealth (1937) 58 CLR 618 (Austl.) ("***Victoria***").
[323] *Cowburn*, *supra* note 295, at 471.
[324] The Factories Act, 1948, No. 63, Acts of Parliament, 1948, § 59.
[325] *Gujarat Mazdoor Sabha*, *supra* note 144, ¶¶ 38-48.

operative part simply directed the Respondent to 'comply with Section 59, without having it to modify the definitional 'minimum wages' to begin with.[326]

Returning to *Cowburn*, the nascent principle and its consequentialist approach for rights were adopted in a few succeeding cases,[327] mostly for circumventing the difficult task of discerning 'implied intent' for the exhaustive field test. The operative words for the argument herein are the terms 'detracted', 'altered',[328] and 'varied'.[329] This brings about a new form of inconsistency: the effect of state modification, as opposed to a quantitative comparison of central and state frameworks, is looked at.[330] This test has had various human rights-related applications in Australian labour-law: Central law permitting female employment while the state law prohibited it through legislation,[331] or where a federal award (law) enabled trade unions to raise funds legislatively prohibited by a state,[332] most illustratively.

Herein, it is argued that a modification of working hours introduces a skewed work hour to wage ratio, which was the object of the Minimum

---

[326] *Id.*, ¶ 50.
[327] Stock Motor Pfoughs Ltd. v. Forsyth, (1932) 48 C.L.R. 128 (Austl.) ("***Stock Motor Pfoughs Ltd.***").
[328] *Cowburn*, *supra* note 295; *Victoria*, *supra* note 322.
[329] *Stock Motor Pfoughs Ltd.*, *supra* note 327, at 196.
[330] Allan Murray Jones, *The Tests for Inconsistency under section 109 of the Constitution*, 10(1) FEDERAL L. REV. 25, 34 (1979).
[331] Colvin v. Bradley Bros. Pty. Ltd. (1943) 68 CLR 151 (Austl.).
[332] Williams v. Hursey, (1959) 103 CLR 30 (Austl.).

Wages Act, the Bonded Labour Act, Articles 23, 39(d), 41 and 42 of the Constitution.

ii. Constitutional Implications on the 2020 Notifications

The Supreme Court's recognition of the 'denial of rights' test is both inexplicit and relatively restricted compared with the one alluded to in the preceding sub-section.[333] However, it does not affect anticipating the judiciary's approving disposition towards the same. A close parallel of the principle is found in *Saverbhai Amaidas v. State of Bombay*,[334] where the state law was concluded to be hit by Article 254(1). The inconsistency being the difference in (degree of) penalty for the same offence, the Supreme Court used a federalised logic of Pillai's contention: it applied Article 254(2) to tacitly repeal the state law, which imposed a higher punishment than the Centre.[335] The Supreme Court discerned an implied repugnancy in a concurrent subject, and applied the constitutional rule of Centre's prevalence.[336]

Similarly, the Supreme Court has inexplicitly applied the denial of rights test in the Indian labour law jurisprudence. For instance, in upholding the Bombay Industrial Relations Act, 1946, the Supreme Court discussed and acknowledged the exhaustive coverage of the subject by the Central law(s).[337] However, since the state law went beyond 'disputes' and also

---

[333] *Id.*, at 607; *Mclean*, *supra* note 302, at 483, 609; O'Sullivan v. Noarlunga Meat Ltd., (1956) 95 CLR 177 (Austl.).
[334] Saverbhai Amaidas v. State of Bombay, (1955) 1 SCR 799.
[335] *Id.*, ¶¶ 6-8; Innoventive Industries Ltd. v. ICICI Bank (2018) 1 SCC 407, ¶ 60.
[336] Hoechst Pharmaceuticals Ltd. v. State of Bihar, (1983) 4 SCC 45, ¶¶ 67, 68.
[337] Ahmedabad Mill Owner's Assn. v. I.G. Thakore, (1967) 2 SCR 437.

provided a novel form of dispute resolution, it had a slicing-edge over the Central law.[338] Applying the obverse of the 'interference with rights' test discussed above, the Supreme Court upheld it to be a valid state exception to the Union laws' completeness.

This test had taken serious shape, if not total recognition, in 1988. In *National Engineering Industries Ltd. v. Shri Kishan Bhageria*, a state legislation was held to be repugnant to the Industrial Disputes Act insofar as it 'curtailed the rights of the workman' by introducing a limitation period.[339] In 2002, a state amendment to the central Industrial Disputes Act was held to be invalid for providing an expanded interpretation of the term 'retrenchment', effectively limiting the right to invoke the Act's protective machinery.[340]

The Indian version, demonstrably, does not necessarily envisage a complete negation of entitlements but only their diminution. The primary requirement seems to be that this entitlement should pre-exist, enacted by either unit of the federation.

It is proposed that the notifications are repugnant by this unrecognised principle. The Central law was enacted embedded with a certain set of stipulation on working hours. The impugned notifications conduce its diminution. Furthermore, the Minimum Wages Act came with its own set of stipulations,[341] that have a certain proportionality with the

---

[338] *Id.*
[339] *Bhageria*, *supra* note 231.
[340] U.P. State Sugar Corpn. Ltd. v. Om Prakash Upadhyay, (2002) 10 SCC 89, ¶¶ 4-6.
[341] *See* The Factories Act, 1948, No. 63, Acts of Parliament, 1948, §§ 51, 52, 54, 56.

hours specified of the former. Reducing work hours is invalid *per se*. A notional wage floor violation is a right-depriving state repugnancy in the federal-concurrent scheme. The denial of rights test applies to both when either's essentiality is reduced.

V. CONCLUSION

The minimum wage rates are predicated upon work hour limits. Work hour limits, like minimum wage workers, enjoy a constitutional protection that no forced subservience may smother.

The cap on working hours and its dynamic proportionality with minimum wages fall precisely in this protected category. This happens for four reasons.

There exists a rule of transference between Parts IV and III of the Constitution of India. There exist several obligations in the former that have their aspirational roots in the latter. Minimum wages are the supposed essence of eliminating undue influence in a relationship such as that of an employer-employee. Hence, a directive suggesting those is taking a fundamental right to its logical conclusion. A government act attempting to retract or violate a legislation is effectively tinkering with a fundamental right.

At the same time, a welfare legislation necessarily enhances human rights. All its prevailing provisions are presumed to be doing the same. Hence, when any one of them is altered so that the previous version of it was more right-enhancing, it is considered constitutionally retrograde.

Lastly, concurrence in legislative jurisdiction implies a marketplace for better legislative ideas in specified fields. In a federation, one unit may appropriate a field or an aspect of it to itself if it deals with it more comprehensively. Working conditions in List III, Schedule VII, seem to enjoy wider Central regulation in the Indian scheme. On the other hand, the incipient denial of rights test considers any right mutilating action of the states to be stillborn. The latter, also a concurrent list concept, shall operate if the concerned right was statutorily provided for earlier. The specified workhours and a proportional set of minimum wages in central laws, are such baseline entitlements.

The entire scheme of the Constitution and the concomitant jurisprudence, therefore, seems to have gauged the prescience in Pillai's words. Invalidating the invocation of Section 5 to dismantle the previous safeguards is constitutionally inevitable. However, the same ought to be the result of considering deprivation of real minimum wages and not by facile considerations such as whether Section 5 found applicability. Any such notification *per se* debilitates the normative ideal emanating from Articles 21, 23, 39, 41, 42 and 254(2) of the Constitution.

NLUJ Law Review

Subhradipta Sarkar, *Impact of Artificial Intelligence in Healthcare in India: Exploring the Issue of Legal Liability*, 8(1) NLUJ L. REV. 90 (2021).

IMPACT OF ARTIFICIAL INTELLIGENCE IN HEALTHCARE IN INDIA: EXPLORING THE ISSUE OF LEGAL LIABILITY

*Subhradipta Sarkar**

ABSTRACT

Healthcare has been one of India's most rapidly expanding industries. Yet the Indian healthcare system continues to be plagued by several problems. On this front, artificial intelligence (AI) provides a promising response to various diagnoses and prognoses. However, it equally presents challenges to patient safety, ascertaining legal liability and data security. Considering the complex technology and large number of actors involved in the AI processes, discovering the fault lines is challenging. Apprehensions are ripe that AI would foster the growth of 'black-box medicines' leading to opaque computational models of decision-making; and hence, creating ambiguity in negligence cases. Efforts are on in building 'explainable AI'. Furthermore, concern remains regarding the 'right to privacy' with regard to the protection of the large amount of healthcare data of patients, especially after the Sprinklr controversy that arose in the context of the Covid-19 patients in Kerala. Notwithstanding the fact that the new Personal Data Protection Bill of 2019 has classified "health data" as

* The author is an Associate Professor of Law at Jamia Millia Islamia, New Delhi and may be contacted at **ssarkar@jmi.ac.in**. The author would like to appreciate and acknowledge the contribution of Mr. Akshay Luhadia, penultimate year student of the West Bengal National University of Juridical Sciences as a Research Assistant for this paper.

"sensitive personal data" and has provided protection, it has also created exceptions for accessing the same. With over 70 per cent of the healthcare in the private hands, acquiring these data sets in developing algorithms and their subsequent sharing raise serious privacy concerns.

TABLE OF CONTENTS

I. INTRODUCTION

Healthcare is one of the most vibrant and growing fields in India. In 2018, the NITI Aayog projected the sector to grow to USD 280 billion by 2020, at an annual growth crossing 16 percent.[342] Nevertheless, it didn't miss to mention the ordeals ranging from acute shortage of qualified professionals to unaffordability, which continues to plague the Indian healthcare system. It is anticipated that Artificial Intelligence [*hereinafter* "**AI**"] and related technologies could be utilized to negate those problems to a large extent.[343]

The potential for AI in healthcare is enormous and it is getting increasingly better at doing human tasks, with greater efficiency and at a lower cost.[344] Specific algorithms have already begun to outdo radiologists in detecting the whereabouts of malignant tumours, and manoeuvre ways for inventing alternatives to expensive clinical trials.[345] AI helps in evaluating information from a particular patient by comparing it with a large dataset from different patients. Correlations are detected and diagnoses are suggested by the self-learning programmes.[346] Yet there are numerous

---

[342] NITI AAYOG, NATIONAL STRATEGY FOR ARTIFICIAL INTELLIGENCE 13 (2018), *available at* https://niti.gov.in/sites/default/files/2019-01/NationalStrategy-for-AI-Discussion-Paper.pdf (last visited May 31, 2021) ("**NITI AAYOG**").
[343] *See generally id* at 24 – 26.
[344] *See* Roland Wiring, *Digitisation in Healthcare: From Utopia to Reality – Artificial Intelligence, Its Legal Risks and Side Effects,* CMS (September 2018), *available at* https://cms.law/en/che/publication/digitisation-in-healthcare-from-utopia-to-reality-artificial-intelligence-its-legal-risks-and-side-effects.
[345] *See* Thomas Davenport and Ravi Kalakota, *The Potential of Artificial Intelligence in Healthcare*, 6 FUTURE HEALTHCARE J 90, 94 (2019).
[346] *See id.*

challenges that lie in front of us before AI-enabled robots replace human doctors. Patients' safety is paramount in medical treatment, and it aims to reduce harm or prevent patients' exposure to risks during provision of health care.[347] Today we are confronted with various issues involving AI which have the potential to threaten patient safety. Till date, AI is not regulated by any specific legislation, so if any diagnosis or surgery goes wrong and results in harm to the patient, there is an uncertainty with regard to civil liability. Who do we hold liable – the AI-provider, the doctor or both?

While the technology promises to deliver quicker and more accurate results, apprehensions are ripe if AI would foster the growth of 'black-box medicines' leading to opaque computational models of decision-making. Their predictions are based on algorithms and not on medical understanding, making their decisions opaque; and hence, creating ambiguity in negligence claims. Additionally, if we seek to regulate AI-based products, there is a need to examine if they qualify as "product liability" under the Consumer Protection Act, 2019.[348] Furthermore, data is at the heart of AI activities. As a result, safeguarding patients' sensitive health data remains a challenge, particularly after the Supreme Court of India [*hereinafter* "**the Supreme Court**"] declared the "right to privacy" a Fundamental Right.[349] The existing legal regime on data protection is regrettably

[347] World Health Organisation, *Patient Safety* (Sep. 13, 2019), *available at* https://www.who.int/news-room/fact-sheets/detail/patient-safety.
[348] Consumer Protection Act, 2019, Act No. 35, Acts of Parliament, 2019 (India).
[349] Justice K.S. Puttawswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

inadequate and the proposed Personal Data Protection Bill, 2019, also poses certain apprehensions. Over 70 per cent of the healthcare expenditure is done by private entities,[350] resulting in large scale presence of the private players in the healthcare sector. As patients visit those private places for treatment, the private entities will resultantly also acquire the patients' data to develop algorithms and become the repository of that data. Consequently, sharing of the data for its usage/storage raises serious privacy concerns.

In this paper, Section II deals with certain basic concepts relating to AI and its implication on healthcare. Section III highlights some major challenges facing Indian healthcare systems and AI initiatives that may go a long way in dealing with these challenges. Section IV elaborates the legal debate in cases of misdiagnosis when patients are treated with the help of AI devices; it delves into the question of negligence, fault-based liability and even the feasibility of drawing strict product liability. As data remains the primary component of AI, protection of patient's data remains a major concern. Therefore, Section V deals with the concerns regarding protection of data. It discusses the legal regime on data protection in India and abroad and draws instances to substantiate the arguments. In Section VI, the author concludes that there are still unsettled issues and thus, endeavours to provide some suggestions towards possible legal solutions.

[350] NITI AAYOG, *supra* note 342, at 26.

II. BASIC CONCEPTS RELATING TO AI AND ITS IMPLICATIONS ON HEALTHCARE

AI entails a variety of algorithms which provide computers the capability to complete tasks which would otherwise require human effort and problem-solving skills. Although AI remains one of the latest trends in the field of engineering, it has been in discussion since 1950s.[351] It was declared as "*the science and engineering of making intelligent machines*" by John McCarthy, one of the founding fathers of AI.[352] To be considered intelligent, according to another AI great, Alan Turing, a computer must be proficient in executing nearly equivalent tasks as a human.[353] AI has been created since then to emulate human reasoning, decision making, knowledge representation, complicated task processing, and exchange of information.[354] AI has also been hailed as the dominant actor for the impending fourth industrial revolution.[355] Stuart J. Russell and Peter Norvig defined AI as a collection of systems with the ability to think, act and rationalise like humans. It's a set of algorithms that allow select machines to operate more efficiently and accurately, emulating human comprehension abilities.[356]

---

351 *See* Sandeep Reddy, John Fox and Maulik P Purohit, *Artificial Intelligence-enabled Healthcare Delivery*, 122(1) J. ROYAL SOC'Y OF MEDICINE 22 (2018) ("**Reddy**").
352 *See id.*
353 *See id.*
354 *See id.* at 2.
355 *See id.*
356 *See* Paulius Cerka, Jurigta Grigiene and Gintare Sirbikyte, *Liability for Damages Caused by Artificial Intelligence*, 30 COMPUTER L & SECURITY REV. 1, 3 (2015) ("**Cerka et al**").

Before we delve into the nuances of the problem at hand, there is a need to highlight a few basic concepts related to AI. Machine learning [*hereinafter* "**ML**"] process is an integral part of AI. Artur Samuel coined the term in 1959 to mean "*the ability to learn without being explicitly programmed*".[357] ML represents that class of machines with the unique capability to shadow human behaviour using aggressive data mining methods such as sensors, metadata input systems and algorithmic protocols, in addition to trailing humans. The ability also accords machines to improvise their functionality sans any overt act by humans.[358]

Deep learning [*hereinafter* "**DL**"] is another important subset of AI. DL is a technique for implementing ML. It offers a technology or network proficiency in data learning that isn't supervised. It acts as a self-sufficient component of AI which works like human brains interconnecting neurons.[359] In fact, Artificial Neural Networks [*hereinafter* "**ANNs**"] are essentially modelled off the biological structure of a brain. The neurons in ANN have distinct layers and are connected with other neurons. A layer is the highest-level building block in DL, which usually obtains weighted input, converts it with a batch of generally non-linear functions and then

---

[357] NITI AAYOG, *supra* note 342, at 14.
[358] *See* Adam Tabriz, *Medico-legal Perils of Artificial Intelligence and Deep Learning*, DATA DRIVEN INVESTOR (Oct. 24, 2019), https://www.datadriveninvestor.com/2019/10/24/medico-legal-perils-of-artificial-intelligence-and-deep-learning/.
[359] *See* NITI AAYOG, *supra* note 342, at 14.

transmits these values as output to the subsequent layer.[360] This very layering has provided deep learning with its name – the more the depth, the greater the learning, which is created by multiple layers.[361] ANN is a complex adaptive system, that means it is capable of altering its inner construction mostly based on the data flowing by it.[362]

III. INDIA'S HEALTHCARE PROBLEMS AND AI APPLICATIONS

NITI Aayog's National Strategy for AI has identified some major deficiencies in our health care sector, *e.g.*, shortfall of qualified healthcare professionals and services compared to World Health Organisation guidelines, wide disparity of healthcare services between urban and rural India, high out-of-pocket expenses making healthcare unaffordable for majority of the population, and reactive approach to essential healthcare.[363]

In such a scenario, it is hoped that greater use of AI would be able to address many of the above-mentioned problems. *E.g.,* in India, while each year new cancer patients grow by more than a million, we have only 2,000 pathologists experienced in oncology.[364] Therefore, large-scale cancer screening possesses a humongous opportunity for AI-induced interventions. ML solutions can assist a general pathologist in performing

---

[360] *See* Academy of Medical Royal Colleges, *Artificial Intelligence in Healthcare* 8 (Jan. 2019), https://www.aomrc.org.uk/wp-content/uploads/2019/01/Artificial_intelligence_in_healthcare_0119.pdf (last visited May 31, 2021).
[361] *See* NITI AAYOG, *supra* note 342, at 13.
[362] *See* Cerka *et al.*, *supra* note 356, at 5.
[363] *See generally* NITI AAYOG, *supra* note 342, at 24 – 26.
[364] *See id.* at 28.

cancer diagnosis and bridge the aforementioned gap.[365] Further, the use of AI is believed to replace current techniques employed by clinicians with greater accuracy, reliability and efficiency.[366] The American Cancer Society has noted that a high number of mammograms produce false positives. Switching to AI allows a 99 percent accuracy along with the process being 30 percent times faster.[367]

Many technology companies which have developed AI applications are significantly revolutionizing the health sector by supporting both patients and healthcare professionals. Several initiatives, both private and governmental, have started in India. NITI Aayog has initiated a partnership with Microsoft in addition to Forus Health to work on eye-check-ups.[368] Max Healthcare claimed that the usage of AI technology drove the cost of critical care down by almost 30 per cent by the efficient use of the ICU ward.[369]

---

365 *See id.* at 29.

366 *See generally* Fei Jiang *et al.*, *Artificial Intelligence in Healthcare; Past, Present and Future*, 2(4) STROKE AND VASCULAR NEUROLOGY 230, (2017).

367 Tejal A. Patel *et al.*, *Correlating mammographic and pathologic findings in clinical decision support using natural language processing and data mining methods,* 123 (1) CANCER 114, 117 (2016); Sarah Griffiths, *This AI Software Can Tell if You're at Risk from Cancer Before Symptoms Appear*, WIRED (Aug. 26, 2016), http://www.wired.co.uk/article/cancer-risk-ai-mammograms (last visited May 31, 2021).

368 *See* NITI AAYOG, *supra* note 342, at 29.

369 *Indian Healthcare is All Set to be Transformed by AI*, MEDICAL BUYER, (Mar. 5, 2019), https://www.medicalbuyer.co.in/indian-healthcare-is-all-set-to-be-transformed-by-ai/.

IV. THE LIABILITY DILEMMA

Nearly all AI solutions currently being developed are not strictly intended to be fully autonomous. The human hand, either directly or through the ability to override the machine, determines, directs, and eventually controls the programming process.[370] Despite all technological developments, AI clinicians comparable to human medical experts appear to be still a distant dream of the future. Nevertheless, the possibility of extensive use of AI tools by the clinicians is real and it presents a daunting task of ascertaining the liability in cases of misdiagnosis or mistreatment.[371]

According to Salmond, the bond of necessity that remains between the wrongdoer and the redress for the wrongdoing is known as liability. It implies the state of a person who has violated the right or acted in contrary to the duty.[372] In other words, the person who is at "fault" is obligated under the tort law to pay damages.[373] Therefore, when a clinician wrongly treats a patient with the approval of the AI diagnostic tool, who becomes liable? The challenge is to ascertain as to where does the fault lies – the clinician or software developer or the medical establishment where the clinician is employed and the AI tool is maintained?

---

[370] *See* Vladeck C. David, *Machines without Principals: Liability Rules and Artificial Intelligence*, 89 WASH. L. REV. 117, 120 (2014).
[371] Anastasia Greenberg, *McGill Intelligence in Health Care: Are the Legal Algorithms Ready for the Future*, MCGILL J. L. AND HEALTH (2017), ("**Greenberg**").
[372] *See* V. D. MAHAJAN, JURISPRUDENCE AND LEGAL THEORY 365 (5th ed., 1987).
[373] Emiliano Marchisio, *In support of "no-fault" civil liability rules for artificial intelligence*, 1 SN SOCIAL SCIENCE 54, 56 (2021) ("**Marchisio**").

A. MEDICAL NEGLIGENCE AND THE DOCTRINE OF *RES IPSA LOQUITUR*

In case of an injury resulting from medical misdiagnosis or mistreatment, liability is derived from the tort of negligence committed by medical professionals. A three-stage procedure must be conformed to assess negligence: (i) the defendant had a "duty of care" towards the plaintiff; (ii) the defendant violated that duty; and (iii) consequently, the plaintiff suffered legally recognised harm. If the plaintiff's case is successful, the defendant will be held liable for damages.[374] The Supreme Court in *Jacob Mathew v. State of Punjab* [375] [*hereinafter* "***Jacob Mathew***"] sought to distinguish between occupational negligence and professional negligence. Adopting a liberal approach, the Supreme Court concluded that a careless attitude, a mistake of judgement or an accident, cannot be said to be a case of medical negligence. Provided that a clinician observes and adheres to the accepted method of the medical profession at the time, he cannot be held liable only since a better therapy exists or a more effective clinician may not have followed the same method.[376] Inability in taking special or unusual steps that might have avoided the actual occurrence cannot be used to judge the suspected negligence.[377]

A clinician can be held responsible for negligence when either he was found unable to perform certain skills which he professed to have or

---

[374] *See* W.V.H. ROGERS, WINFIELD AND JOLOWICZ ON TORT 150 (18th ed., 2010).
[375] Jacob Mathew v. State of Punjab, A.I.R. 2005 S.C. 3180.
[376] *See id.* at ¶ 49(2).
[377] *See id.*

he did not proceed with the due diligence required of a prudent man. It's a utopian idea for every professional to command the highest degree of knowledge or skill in the area of his practice. Hence, the standard for judging negligence of an individual, might be that of a professional individual in that field performing standard tasks.[378] The method depends on finding faults caused by the doctor, hospital, and others to ascertain medical negligence. The plaintiff must prove on the basis of probability that the hospital or doctor (the defendant) was negligent.[379]

In cases of negligence, *prima facie*, it is for the plaintiff to satisfy the courts that the harm has happened due to the defendant's negligence. However, in many cases it has been difficult for the plaintiff to adduce enough evidence about negligence to sustain his/her claims.[380] To obviate such a hardship, a presumption is required to be made about the factum of negligence in the happening of an unfortunate accident in view of the evolution of the doctrine of "*res ipsa loquitur*". The doctrine refers to an implication of negligence being drawn against the defendant as a result of the occurrence of certain events.[381]

In *Lloyde v. West Midlands Gas Board*,[382] Megaw L. J. explains that as the plaintiff *prima facie* establishes negligence as per this doctrine when, (a) he cannot exactly explain the relevant act or omission that gradually led to

---

[378] *See id.*
[379] *See* Daniele Bryden and Ian Storey, *Duty of care and medical negligence Continuing Education in Anaesthesi*a, 11(4) CRITICAL CARE & PAIN J. 124, 124 (2011).
[380] *See* JOHN MURPHY, STREET ON TORTS 249 (2007).
[381] Manubhai Punamchand Upadhya v. Indian Railways, 1997 A.C.J. 1270, ¶14.
[382] Lloyde v. West Midlands Gas Board, (1971) 2 All E.R. 1240.

the accident; and (b) the potent cause of the accident was any act or omission of the defendant or another person for whom the defendant is responsible, according to the evidence as it stands at the relevant time.

Indian courts have employed this doctrine in medical negligence cases. In the famous case of *Mrs. Aparna Dutta v. Apollo Hospital Enterprises Ltd.*,[383] the plaintiff was subjected to an operation (in the defendant's hospital) for removal of her uterus, as she was diagnosed to have cyst in one of her ovaries. After the operation, she continued to suffer from severe pain, she had to, unfortunately, undergo another surgery to get the abdominal pack removed which was left by the first surgeon. In an action claim of negligence, the court determined that leaving a foreign matter in the body during the procedure was a case of *res ipsa loquitur* as no other explanation for the presence of the abdominal pack is plausible.[384] The plaintiff was paid compensation.

We are still in the nascent stages of using AI and the medical community is yet to lay down any acceptable protocols involving AI tools. Unless such protocols are laid down, given the *Jacob Mathew* judgement, it would be extremely difficult for the judges to decide if the clinician in question is negligent. Under the existing medico-legal liability regime, often the traces of liabilities are ambiguous when medical errors occur; and it would become even more debatable when more and more autonomously designed AI 'agents' start delivering healthcare services.[385] In such cases,

---

[383] Mrs. Aparna Dutta v Apollo Hospital Enterprises Ltd, A.I.R. 2000 Mad. 340.
[384] *See id.* ¶ 23.
[385] *See* Reddy, *supra* note 351, at 4.

applying the doctrine of "*res ipsa loquitur*", a presumption of liability on the part of the clinicians and/or hospitals may be derived. They may be held liable for failing to take the necessary precautions before deploying AI tools or procedures to treat patients.

B. PRODUCT LIABILITY AND ITS LIMITATION

Some experts feel that the claims and success of AI are overblown. In recent times, the outcome of the accidents involving Tesla's semi-autonomous cars in the United States is relevant to that point. It has important ramification on the question of liability involving AI tools in healthcare. Because Tesla had been aggressively advertising about their cars' full self-driving capabilities, drivers over-relied on the ability of those cars and did not take active participation in the driving or they remained distracted, *e.g.*, playing cell phone games in one case. In the exemplified case in 2018, the driver died when his car, in auto-pilot mode, hit a concrete barrier on a Silicon Valley Freeway.[386] Eventually, the National Transportation Safety Board [*hereinafter* "**NTSB**"] found that the cars in question had limitations on self-driving mode with respect to driver distraction, level of driver engagement and collision avoidance system. However, the regulators failed to take note of the limitations of safety measures built in those cars. The NTSB found the victim-driver negligent in the act and held Tesla only partially liable for the accidents and

[386] *See* Rebecca Heilweil, *Tesla Needs to Fix Its Deadly Autopilot Problem,* VOX (Feb. 26, 2020), https://www.vox.com/recode/2020/2/26/21154502/tesla-autopilot-fatal-crashes.

recommended for more oversight of such cars by appropriate authorities.[387] In the absence of fully AI-driven clinicians or programmes, it is the humans who either manage them or eventually act on the diagnoses. Therefore, in a comparable situation we can say that the operator/clinician will most probably be held liable for any resultant harm.

There are certain inherent problems with AI usage in healthcare, especially in the realm of legal liability. ML has the ability to intake intricate data consisting of millions of gigabytes. Algorithms are trained to generate classifications or predictions using statistical approaches and improvise the machines.[388] The higher the complexity of the data which the machine is trained on, the better and more accurate results it can produce. In fact, there has been a rapid increase in the collection of health data today than ever before. Gradual transition of this data in electronic form, known as 'Electronic Health Records' [*hereinafter* "**EHRs**"], has served a variety of reasons: from enhancing efficiency in patient care to maintaining records for settling insurance claims and preventing malpractices.[389] Nonetheless, there's a danger of 'overfitting'. It happens when algorithms learn modelling datasets to an extent that it can't efficiently simplify on a new dataset – one

---

[387] *See Collision Between a Sport Utlity Vehicle Operating with Partial Driving Automation and a Crash Attenuator Mountain View, California*, National TRANSPORT SAFETY BOARD (Mar. 23, 2018), https://www.ntsb.gov/news/events/Documents/2020-HWY18FH011-BMG-abstract.pdf.

[388] *See* Reddy, *supra* note 351, at 2.

[389] *See* W. Nicholson Price II, *Black-Box Medicine*, 28(2) HARVARD J. L. & TECH. 419, 430 – 31 (2015) ("**W. Nicholson Price II**").

used in making decisions about new patients.[390] For example, any ML trained on data that over-represents white patients, may give the wrong diagnosis regarding coloured patients.[391] Hence, diligent ML researchers consistently find new types of data problems or sets for their machines to analyse the reliability of the machine and just how generalizable their machines are. Error, although, as in humans, is inevitable.[392] Such may lead to a case of misdiagnosis.

i. Inexplicability Surrounding Black-box Medicines

The introduction of AI will lead to the growth of "black-box medicine" which are principally based on opaque computational models. In AI systems, input data and output decisions are known, but exact steps taken by the computer and software to reach the decision cannot always be fully retracted. This process is known as "black box".[393] As the name suggests, the machine is learning about the data patterns rather autonomously. Even the developers of the AI systems are ignorant about the process of reaching the conclusions by the systems.[394] One of the defining characteristics of black box medicine is that it cannot explain its

---

[390] *See* Jason Brownlee, *Overfitting and Underfitting with Machine Learning Algorithms*, MACHINE LEARNING MASTERY, (Mar. 21, 2016), https://machinelearningmastery.com/overfitting-and-underfitting-with-machine-learning-algorithms/.

[391] *See* Olivia Goldhill, *When AI in healthcare goes wrong, who is responsible?*, QUARTZ (Sep. 20, 2020), https://qz.com/1905712/when-ai-in-healthcare-goes-wrong-who-is-responsible-2/ ("**Goldhill**").

[392] *See* Greenberg, *supra* note 371, at 7.

[393] *See generally* W. Nicholson Price II, *supra* note 389, at 2.

[394] *See* Liz Szabo, *A Reality Check on Artificial Intelligence: Are Health Care Claim Overblown*, KHN (Dec. 30, 2019), https://khn.org/news/a-reality-check-on-artificial-intelligence-are-health-care-claims-overblown/.

findings; in that way it is non-transparent. It does not base its findings on sound medical knowledge, rather its purely a prediction based on the working of an algorithm.[395] To neutralize this problem, researchers are trying to develop "explainable AI" which are ML algorithms that are inherently explainable. Thus, "explainability" can explain how decisions are drawn, allowing for better future decision-making as well as inspection and traceability of AI behaviour. Humans will be able to get into AI decision loops and stop or monitor their tasks as required thanks to traceability. An AI system is supposed to not only complete a task or make decisions, but also provide a model that can include a clear report on why it reached those conclusions.[396]

Gabriela Bar, an expert in the law of new technologies, suggests AI systems should be explainable by design. She refers to European Commission's White Paper on Artificial Intelligence of 2020 which emphasises that future AI regulatory framework should include the types of legal obligations to be imposed on entities involved in all stages of AI operations from designers to end-users.[397] However, the transparency of AI operations and the explainability of its decisions can be a calibrated one as all entities involved do not require the same kind of information as to how

---

395 *See* Susan Athey, *Beyond Prediction: Using Big Data for Policy Problems*, 355(6324) SCIENCE 483, 485 (2017).

396 *See* Ron Schmelzer, *Understanding Explainable AI*, FORBES (Jul. 23, 2019), https://www.forbes.com/sites/cognitiveworld/2019/07/23/understanding-explainable-ai/?sh=264ef6f47c9e.

397 *See* Gabriela Bar, *Explainability as a legal requirement for Artificial Intelligence*, MEDIUM (Nov. 27, 2020), https://medium.com/womeninai/explainability-as-a-legal-requirement-for-artificial-intelligence-systems-66da5a0aa693.

raw data and code translate into benefits or harms. Moreover, there could be intellectual property rights issues, so it is not always possible or necessary to explain the working of the AI completely. Nevertheless, there could be high-risk AI, *e.g.*, used in the healthcare sector, where such trade-offs should commensurate with risk assessment and the its impact on human life. In effect not only will public confidence in AI grow, but it will also assist us to ascertain appropriate liability in AI operations.[398]

On one hand, for competitive purposes, AI is deliberately hidden but on the other hand, some techniques are just above human understanding. ML technologies can be particularly opaque because they have the ability to adjust themselves through various small tweaks which change their parameters and the rules by which they operate. This causes issues when it comes to validating outputs for AI systems and detecting errors or biases in the data.[399] The House of Lords Select Committee on AI has already forewarned that the datasets available to machines do not properly represent the wider population and therefore could lead to prejudiced or unfair decisions that would further cause chaos.[400] IBM released an IBM Watson Oncology machine for diagnosing cancer. However, its use was halted in clinics because outside the US, doctors did not believe in its recommendations. They felt that the database used for

---

398 *See id.*

399 *See* Ran Svenning Berg, *Artificial Intelligence in Healthcare and Research,* NUFFIELD COUNCIL ON BIOETHICS, (May 15, 2018), https://www.nuffieldbioethics.org/publications/ai-in-healthcare-and-research.

400 *See id.*

cancer treatment was very American-oriented.[401] In such ambiguous cases, it's unclear where the fault ought to lie in case of any harm – whether with the ML company who collected biased data or the clinician who acted upon that recommendation.[402] Both the manufacturer and operator may be jointly held liable for any resultant damage suffered by the patient. The share of the burden may be determined by the judiciary on a case-to-case basis.

ii. Faculty Medical Devices and their Consequences

AI tools or programmes are designed or developed by another person and misdiagnosis or mistreatment may occur due to a faulty device. This could be beyond the know-how of the clinician, and hence, it brings us to the next probability, *i.e.,* the liability of the software developer or manufacturer for the flaws in manufacturing, design, or programming which might have caused the injury. This option would lie in the realm of product liability. Product liability also infers a certain onus on the manufacturer or vendor of the goods to compensate the injured due to defective merchandising that was available for sale.[403] The issues of product-liability have also led to the introduction of certain contract principles and tort principles as well. Here, the contract principle is based on 'warranty' whereas tort law product liability is propounded from

---

401 *See id.*

402 *See generally* Goldhill, *supra* note 391.

403 *See* Anindya Ghosh and Nabarun Chandra Ray, *India: Product Liability Law in India: An Evolution*, MONDAQ (Aug. 7, 2020), https://www.mondaq.com/india/dodd-frank-consumer-protection-act/974270/product-liability-law-in-india-an-evolution ("**Ghosh and Ray**").

'negligence' and 'strict liability'.[404] Through the passage of time, product liability jurisprudence has advanced along the lines of adjudging the manufacturer responsible for damages in cases of harm suffered by the eventual consumer as a result of a manufacturing error, despite the fact that there was no arrangement between the consumer and the manufacturer.[405]

Since AI is so recent with many unknown threats, it needs close monitoring. Yet the reality is juxtaposed. In a technologically advanced country like the United States, the majority of AI devices are exempted from US Food and Drug Administration [*hereinafter* "**FDA**"] approval.[406] Furthermore, the Nationwide Academy of Medicine asserts that there's been no serious analysis on whether 320,000 medical applications available today really enhance health.[407] Many of these application developers have never applied for FDA clearance, despite the fact that it is legally required. Furthermore, with subtle backing from the business lobby, legislative changes have been introduced to exempt countless medical software programmes from federal review, along with health apps, digital well-being information and instruments that assist doctors in making medical decisions.[408] For instance, in 2016, the Federal Food, Drug, and Cosmetic

---

[404] *See* VIVIENNE HARPWOOD, MODERN TORT LAW 335 – 36 (6th ed., 2005); *see also Products liability*, LEGAL INFORMATION INSTITUTE (CORNELL LAW SCHOOL), https://www.law.cornell.edu/wex/products_liability (last visited May 31, 2021).
[405] *See* Ghosh and Ray, *supra* note 403.
[406] *See Changes to Existing Medical Software Policies Resulting From Section 3060 of the 21st Century Cures Act*, FDA (Sep. 2019), https://www.fda.gov/regulatory-information/search-fda-guidance-documents/changes-existing-medical-software-policies-resulting-section-3060-21st-century-cures-act ("**FDA**").
[407] *See* Szabo, *supra* note 394.
[408] *See id.*

Act [*hereinafter* "**FD&C Act**"] was amended by the 21st Century Cures Act to removed certain software functions from the definition of 'device' under the FD&C Act.[409] Faulty or unregulated AI devices or programmes can wreak havoc. In recent years, the FDA has come under fire from various quarters, including the American Medical Association, for allowing hazardous medical devices to be sold, which the Consortium of Investigative Journalists has linked to nearly 80,000 fatalities and 1.7 million injuries over the last decade.[410]

Johnson & Johnson [*hereinafter* "**J&J**"] hip implant fiasco is well documented. Faulty hip implants manufactured by the company forced thousands of patients to undergo revision surgeries. Eventually the company was forced to recall the implants worldwide and pay millions of dollars in compensation.[411] Indian patients also suffered the brunt of the problem. The Government set up an expert committee at both the centre and state-levels. It was found that J&J suppressed the fact of the adverse effects of such faculty hip implant from the regulators. In India, based on the recommendation of the expert committees, the Central Drugs Standard Control Organisation [*hereinafter* "**CDSCO**"], equivalent to the US FDA,

---

409 FDA, *supra* note 406.
410 *See* Szabo, *supra* note 394.
411 *See generally* Kaunain Sheriff M, *How Johnson and Johnson Hip Implants System Went Wrong*, THE INDIAN EXPRESS (Aug. 30, 2018), https://indianexpress.com/article/explained/johnson-and-johnson-how-hip-implants-went-wrong-jp-nada-5331779/.

directed J&J to pay INR 7.5 lakh compensation to the first patient from Mumbai in 2019.[412]

iii. Scope of Product Liability under Consumer Protection Act, 2019

It is noteworthy that the new Consumer Protection Act, 2019 [*hereinafter* "**CPA**"][413] has specifically incorporated the aspect of product liability. According to Section 2(34) of CPA,[414] "product liability" refers to the responsibility of a product manufacturer or seller to pay compensation for any harm caused to a customer because of any defective product or deficient service. A pertinent question may further arise as to whether ML incorporated into software itself counts as "product" under CPA? Under Section 2(33) of the CPA[415] "product" includes any article or goods or extended cycle of such product, possessing intrinsic value that can be delivered either as wholly assembled or as a component part and produced for commercial purposes.

It appears that the existing definition coupled with the inherent opacity of AI software (as standalone product) may be challenging to establish liability under the CPA. However, if AI software is implemented

---

[412] *See CDSCO Directs Johnson & Johnson to Pay Rs. 74.5 Lakh to First Patient With Faulty Hip Implant*, WIRE (Mar. 13, 2019), https://thewire.in/health/cdsco-directs-johnson-johnson-to-pay-rs-74-5-lakh-to-first-patient-with-faulty-hip-implant.
[413] Consumer Protection Act, 2019, Act No. 35, Acts of Parliament, 2019 (India) ("**CPA**").
[414] CPA, § 2(34).
[415] CPA, § 2(33).

into devices to make it a composite product (*e.g.*, a blood glucose monitor) and it fails, the manufacturer of such product may be held liable.[416]

C. RELEVANCE OF STRICT PRODUCT LIABILITY

It appears that because of the complexity of the AI programmes and difficulty in determining as to where exactly the fault lies, ordinary liability principles may fall short. Yet they hold inherent potential in causing considerable harm. This calls for a special situation, *i.e.*, strict liability, where if the products are defective to a great extent and dangerous, the seller/manufacturer shall bear the responsibility for any loss or personal injury. In such a scenario, the law stipulates a defendant to compensate the claimant's loss even if he was not at fault. Nevertheless, it is not an absolute principle as there may be disclaimers on product liability, a recovery cap, or the economic damage may not be recoverable.[417]

Over the last century, courts have found that proving injury cases against manufacturers and vendors was arduous for critically injured consumer claimants. In *Escola v. Coca-Cola Bottling Co.*,[418] a case where an explosion of a Coca-Cola bottle caused injury, the Supreme Court of California decided in favour of the plaintiff by employing the doctrine of *res ipsa loquitur*. However, in the concurring judgement Justice Roger Traynor observed that instead of relying on the principle of negligence, the manufacturer should have incurred "absolute liability" for placing an article

---

[416] Johan Ordish, *Legal liability for machine learning in healthcare*, PHG Foundation, (Aug. 2018), https://www.phgfoundation.org/media/217/download/briefing-note-legal-liability-for-machine-learning-in-healthcare.pdf?v=1&inline=1.
[417] *See* Ghosh and Ray, *supra* note 403.
[418] *See* Escola v. Coca Cola Bottling Co., 24 C2d 453 (1944).

in the market which he knew would be sold without inspection, and that proved to have a defect causing injuries to others.

Subsequently, in the case of *Henningsen v. Bloomfield Motors, Inc.*,[419] the plaintiff bought a car from the defendant's dealership. The express warranty was only to replace the defective parts. However, the plaintiff's wife met with an accident because the steering had malfunctioned. The plaintiff filed a lawsuit against both the dealer and the auto maker. The defendants declined to pay for repairing the vehicle under warranty because they claimed their warranty only covered defective parts and were not liable for any damage caused by defective parts. The New Jersey Supreme Court rejected this claim and granted Henningsen damages, reasoning that the sale of each item was accompanied by an implicit guarantee of protection.

The principle has received some mentioning in India in the case of *Airbus Industries v. Laura Howell Linton*,[420] where deaths and injuries were caused due to a faulty landing of an aircraft. When the defendants argued that Indian law did not have strict product liability, the Karnataka High Court retorted that merely because Indian courts haven't enunciated such a principle, parties could not go without any remedy. It was observed that if required, a new principles would be brought in to remedy such situations as was done in *Charan Lal Sahu v. Union of India*[421] in the aftermath of the Bhopal Gas Tragedy.

---

[419] *See* Henningsen v. Bloomfield Motors, Inc., 32 N.J. 358 (1960).
[420] *See* Airbus Industries v. Laura Howell Linton, I.L.R. 1994 Kar. 1370.
[421] *See generally* Charan Lal Sahu v. Union of India, A.I.R.1990 S.C.1480.

Although this principle hasn't found a place in the CPA, it deserves mentioning that Section 87 of the Act[422] lays down certain specific exceptions to product liability. However, those exceptions do not specifically address the situations that are being discussed in this paper.

Nevertheless, the application of strict product liability principle to AI can be complicated. In this area, the cause-and-effect relationship, as it relates to the causality of the injury, may not be linear. An AI technology designer cannot necessarily foresee how the technology will act once it is being used in a real-world medical setting. Furthermore, even though there are no bugs in the design or its execution, the results can be unpredictable. As many entities and individuals, such as designers, engineers, and developers, work together to create an AI technology and its systems, it makes it extremely difficult to pinpoint the "fault" and blame any single individual.[423]

There is another downside to imposing strict liability. This could expose producers and programmers to volatile and potentially limitless civil liability lawsuits, with no way to mitigate the risks by raising safety investments because the harm could be unforeseeable. Hence, AI designers could be reluctant to indulge in research to their full potential and it could eventually hamper technological progress.[424]

---

[422] CPA, § 87.
[423] *See* Marchisio, *supra* note 372, at 61.
[424] *See generally id.*, at 62 – 63.

In such a scenario, a possibility arises of conferring AI tools/programmes with a 'legal personality' or in other way treating them as robots.[425] Then such robots will have the legal status compared to human clinicians and may be sued for any damage caused due to their actions. The operator/clinician may opt for compulsory insurance cover so that any claims arising out of its use can be paid out of the insurance. Further, the insurance itself may have a cap so that there is no limitless liability on the insurance company either. However, all this may only be made possible through appropriate legislation in this regard.

V. LIABILITY REGARDING PROTECTION OF PERSONAL HEALTH DATA

As mentioned earlier, there has been a gradual progression to EHRs, which keep health data in electronic form rather than in physical files. Such a trend has aided the massive development of recorded data. It has also raised the concern of the safety and privacy of EHRs. Since data is at the core of AI-driven health systems, a few fundamental concerns about health data ownership, use, and accountability in the event of data misuse or unauthorised use must be addressed. Confidential and private data will be used in AI healthcare applications. There have been cases of substantial violations both in India and abroad which further emphasise the need to fix liability in such situations.

---

[425] *See generally* Mariam Mgeladze and Murman Gorgoshadze, *Applicability of Legal Regulations to High Artificial Intellect - Robots*, 2019 J. Const. L. 51 – 72 (2019).

A. INSTANCES OF VIOLATION OF PATIENTS' DATA

In 2017, a major controversy sparked when London-based Royal Free National Health Service Foundation Trust floundered in adhering to the data privacy laws when it revealed 1.6 million patient records to Google-owned AI firm DeepMind for a trial. Investigation in this matter revealed that as part of the trial, the Trust did not inform patients about the extent of usage of their details. It struck a deal with Google and shared patient's sensitive personal data, *e.g.*, HIV status, mental health history and abortions, without their express consent. The Information Commissioner's Office held that the deal was a serious violation of the right to privacy and ordered for tighter guidelines. However, it did not penalise the Trust financially. Both the Trust and DeepMind admitted the breach and committed themselves to stricter norms.[426]

Recently, a similar data privacy infringement took place in the State of Kerala. The state government contracted with Sprinklr, a US-based tech firm, for the management of personal information of COVID-19 patients, and allegedly gave access to data of 175,000 people of Kerala without their "informed consent".[427] The opposition party in the state called for the cancellation of the agreement and sought the intervention of the High

---

[426] *See* Alexander J Martin, *NHS patients' data was illegally transferred to Google DeepMind*, SKY NEWS (Jul. 7, 2017), https://news.sky.com/story/nhs-patient-data-given-to-google-illegally-10935315.

[427] *See* Anil S, *Sprinklr row: Controversy which blotted the COVID-19 clean slate of Kerala Government*, INDIAN EXPRESS, (Apr. 26, 2020), https://www.newindianexpress.com/states/kerala/2020/apr/26/sprinklr-row-controversy-which-blotted-the-covid-19-clean-slate-of-kerala-government-2135352.html.

Court as such data breach amounts to the violation of right to privacy under Article 21 of the Constitution of India.[428] The High Court also did not appreciate the state's decision for choosing the jurisdiction of the courts in New York and that the agreement was finalized without sanction of the Law Department.[429] In order to ensure that there is no "data epidemic" after the COVID-19 is contained, in an interim order, the High Court in *Balu Goplalakrishnan v. State of Kerala* [*hereinafter* "***Sprinklr case***"] issued certain directions which include:[430]

a) The state government requires individuals to provide informed consent for their data to be handled by a third-party foreign corporation.
b) The state should only allow Sprinklr to access anonymised data.
c) Sprinklr was restrained from exploiting any data for commercial purposes.
d) Sprinklr should respect the confidentiality and return the entire data to the state after its contractual obligations are over.

---

[428] *See Sprinklr Deal: Kerala HC Seeks Govt Explanation on Foreign Jurisdiction Clause and Lack of Law Dept. Sanction*, LIVELAW NEWS NETWORK (Apr. 21, 2020), https://www.livelaw.in/news-updates/sprinklr-deal-kerala-hc-seeks-govt-explanation-on-foreign-jurisdiction-clause-and-lack-of-law-dept-sanction-155559; *see also Balu Gopalakrishnan v. State of Kerala and Ors.*, GLOBAL FREEDOM OF EXPRESSION (COLUMBIA UNIVERSITY), https://globalfreedomofexpression.columbia.edu/cases/balu-gopalakrishnan-v-state-of-kerala-and-ors/.

[429] Balu Goplalakrishnan v. State of Kerala, W.P.(C). Temp. No. 84 of 2020, ¶ 1. ("***Sprinklr case***").

[430] *See id.*, at ¶ 24.

Facing flacks from all corners, the Government of Kerala eventually cancelled the deal with Sprinklr and informed the High Court about the same.[431]

B. DRAWING INSPIRATION FROM EUROPEAN UNION'S GENERAL DATA PROTECTION REGULATION

The European Union's [*hereinafter* "**EU**"] data protection legal regime, the General Data Protection Regulation [*hereinafter* "GDPR"], is considered as one of the developed data protection models,[432] and it applies to all EU member states as well as all organisations that hold and process personal data about EU residents, regardless of where they live. In other words, GDPR has an impact on data protection requirements globally. Failure to comply with the requirements prescribed under the GDPR attracts stiff penalties to the extent of € 20 million or 4 per cent of the corporation's annual global revenue, whichever is greater. It may also be mentioned that it has served as a model for many countries outside the EU, including India, to draft their own laws.[433]

---

[431] *See generally* Jeeman Jacob, *Kerala Backs Out of Sprinklr Deal, Cancels Controversial Pact Over Privacy Issues*, INDIA TODAY, (May 21, 2020), https://www.indiatoday.in/india/story/kerala-sprinklr-deal-covid-19-pinarayi-vijayan-high-court-1680484-2020-05-21.

[432] *See generally* Lakshya Sharma and Siddharth Panda, *Into the Orwellian Dystopia: A Comparative Analysis of Personal Data Protection Bill 2019 vis-à-vis Indian Privacy Jurisprudence*, 7(2) NLUJ L. REV. 1, 15 – 17 (2021) ("**Sharma and Panda**").

[433] *See generally* Juliana De Groot, *What is the General Data Protection Regulation? Understanding & Complying with GDPR Requirements in 2019*, DIGITAL GUARDIAN (Sep. 30, 2020), https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection.

The GDPR's core privacy and data protection provisions include the following:[434]

a) No data processing without the subjects' permission;
b) Collected data to be anonymised for maintaining privacy;
c) Notifying data principals about data breaches;
d) Ensuing safety in transferring of data across borders; and
e) Appointment of data protection officers by certain companies to supervise GDPR compliance.

According to a study commissioned by the European Commission, GDPR has a bearing on AI-powered mobile health applications. Accordingly, operating systems and device manufacturers, third parties (*e.g.*, advertisers), mobile-health app developers, etc., must comply with privacy rights and abide by the concept of necessity and proportionality. Use of anonymised data or at least the use of pseudonymised data should be favoured. The use of non-pseudonymised data should be reduced as much as possible.[435]

It highlights that the concept of consent is crucial in healthcare beyond data protection as a component of the patient's self-determination. The study reveals that patients will not normally have access to the application unless they agree to the rules of the mobile health app. Further,

---

[434] *See id.*

[435] *See* C. HOLDER *ET AL.* (EDS.), LEGAL AND REGULATORY IMPLICATIONS OF ARTIFICIAL INTELLIGENCE: THE CASE OF AUTONOMOUS VEHICLES, M-HEALTH AND DATA MINING 19 (2019), https://publications.jrc.ec.europa.eu/repository/bitstream/JRC116235/jrc116235_report_on_ai_%281%29.pdf.

availability of the information only in English creates a hindrance for the patients to give informed consent.[436]

The study report stated that if the AI medical devices are covered under EU Regulation 2017/745 on medical devices, then they are required to conform with CE markings,[437] information duties, etc,[438] making the producers liable for causing any harm; however, it was found most of them are unaware of such regulations.[439] The producer/owner of the AI software/product is forced to adopt a privacy by design approach[440] and would be liable under the GDPR for any breach of privacy. In case the producer and operator are two different entities, the GDPR might fall short. Since GDPR only applies to data controllers and processors, it does not apply to companies who still generate software that processes personal data. In this situation, the producer and operator's current contractual arrangement should be examined. This contract should fix the duties of the producer. Companies using software produced by a third party should highlight the same in their contracts.[441]

---

[436] *See id.*, at 20.
[437] The CE marking (an acronym for the French "Conformite Europeenne") certifies that a product complies with EU health, safety, and environmental regulations, ensuring safety of consumers. *See Certifying Your Product with CE Marking,* INTERNATIONAL TRADE ADMINISTRATION, https://www.trade.gov/ce-marking (last visited May 31, 2021).
[438] *See id.*, at 23.
[439] *See id.*
[440] The European General Data Protection Regulation 2016/679, art. 25(1).
[441] *See id.*, at 24.

C. INDIA: RIGHT TO PRIVACY AND PERSONAL DATA PROTECTION BILL, 2019

Unlike the EU, India lacks an extensive law dealing with personal data security. The Information Technology Act, 2000[442] [*hereinafter* "**IT Act**"] was initially enacted to make internet commerce easier by granting legal status to electronic transactions. However, it was amended in 2008[443] to include, *inter alia*, provisions for protection of data collected, processed or stored electronically.[444] Currently, the data protection regime is governed by the IT Act read with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011[445] [*hereinafter* "**IT Rules**"] framed under Section 43A of the Act.[446] The legal framework mandates that a "body corporate" must protect "sensitive personal data or information" when providing any service or performing under a contract, adhere to certain standards, and pay compensation to the affected person in the event of a "intentional personal data breach" under Section 72A of the IT Act.[447] Such information includes "medical records and history".[448] The body corporate is obligated to

---

[442] Information Technology Act, 2000, Act No. 21, Acts of Parliament, 2000 (India) ("**IT Act**").
[443] Information Technology (Amendment) Act, 2008, Act No. 10, Acts of Parliament, 2009 (India).
[444] PRS Legislative Research, *Rules and Regulation Review: The Information Technology Rules*, 2011, PRSINDIA (Aug. 12, 2011), https://prsindia.org/files/bills_acts/bills_parliament/2011/IT_Rules_and_Regulations_Brief_2011.pdf.
[445] Ministry of Communications & Information Technology (Department of Information Technology), Notification No. G.S.R. 313(E) (Apr. 11, 2011).
[446] *See* IT Act, § 43A.
[447] *See* IT Act, § 72A.
[448] *See* IT Rules 2011, r. 3.

provide a privacy policy and to be available to the data owner,[449] who shall give informed consent about the purpose for such collection but can withdraw his earlier consent.[450] Although the consequences of such withdrawal are noted under the IT Rules, it can logically be deduced that this will lead to the erasure of data by the corporate.[451] Every corporate is to designate a grievance officer for addressing any discrepancies and grievances expeditiously within one month of their receipt.[452]

The IT Rules further provide that, save in the case of a legal (or statutory) duty, a body corporate must get the prior authorization of the supplier of sensitive personal data before disclosing such data to any third party.[453] Any data processor will be presumed to have complied with the IT Rules if it has met the relevant international standard mentioned therein or its equivalence approved by the Central Government.[454]

Personal health data is part of our right to privacy whose protection has been deliberated in various judgements of the Supreme Court,[455] culminating into *Justice K. S. Puttaswamy (Retd.) v. Union of India*, [*hereinafter* "***Puttaswamy***"][456] where the Court held "right to privacy" as part of the

---

[449] *See id.*, r. 4.
[450] *See id.*, r. 5.
[451] *See* Vinod Joseph, Protiti Basu and Ashwarya Bhargava, *India: A Review of The Information Technology Rules, 2011: Reasonable Security Practices and Procedures and Sensitive Personal Data or Info*, MONDAQ (Mar. 19, 2020), https://www.mondaq.com/india/privacy-protection/904916/a-review-of-the-information-technology-rules-2011-.
[452] *See* IT Rules, 2011, r. 5(9).
[453] *See id.*, r. 6.
[454] *See id.*, r. 8.
[455] *See generally* Sharma and Panda, *supra* note 432, at 18 – 21.
[456] Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1.

right to life and personal liberty as enshrined under Article 21 of the Constitution of India. Although the Supreme Court held that the right is not an absolute guarantee, the invasion of one's privacy whether by a private or public actor must pass the triple test, *i.e.*, (a) legitimate aim, (b) proportionality, and (c) legality. The directions issued by the Kerala High Court in *Sprinklr case* provides further protection to the health data.

Rapid development in technology left many aspects unaddressed through the existing law, and drawing impetus from the GDPR, the Government presented Personal Data Protection Bill, 2019 [*hereinafter* "**PDP Bill**"],[457] before the Lok Sabha on December 11, 2019, and subsequently referred it to the Standing Committee in the pursuit of enacting the legislation.[458] The PDP Bill regulates personal data processing by the government, Indian corporations, and international corporations. As per the PDP Bill, "personal data" refers to information about an individual's features, qualities, or attributes of identity that can be used to classify them.[459] Further, it classifies "health data" as "sensitive personal data".[460]

The PDP Bill allows for a data fiduciary, whether in the case of a natural or legal individual, to process personal data under certain conditions, including purpose, processing, and storage limitations. Personal

---

[457] Personal Data Protection Bill, 2019, Bill No. 373, Bills of Parliament, 2019 (India).
[458] PRS Legislative Research, *The Personal Data Protection Bill, 2019*, PRSINDIA, https://www.prsindia.org/billtrack/personal-data-protection-bill-2019 (last visited May 31, 2021).
[459] *See* Personal Data Protection Bill, 2019, cl. 2(28).
[460] *See id.*, cl. 2(36).

data processing, for example, should not be permitted unless there is a specific, clear, and lawful reason for doing so. Accordingly, the data fiduciaries are obligated towards ensuring transparency and accountability, together with instituting grievance redressal mechanisms dealing with individual complaints.[461] It further requires substantial data fiduciaries that handle sensitive personal data to complete a data security review before proceeding with any procedure involving the use of emerging technology, extensive profiling, or the use of sensitive personal data.[462]

The PDP Bill envisions the data principal having a number of rights, including the right to seek assurance from the fiduciary regarding collection of their personal data, the right to restrict continued disclosure of such data by a fiduciary, data correction and erasure, data portability, and so on.[463] It also aims to clarify different aspects of consent that are relevant for the processing of personal data.[464] The PDP Bill does, however, list the grounds for collecting personal data without permission, which include reacting to any medical emergency arising from a life threat or a serious health compromise of the data subject or any other individual.[465] This gives the state a scope to process our personal health data in situations like the COVID-19.

It is far-fetched to expect citizens in a nation like India, where poverty and illiteracy have completely disenfranchised them, to be able to

---

461 *See id.*, chap. II.
462 *See id.*, cl. 27.
463 *See id.*, chap IV.
464 *See id.*, cl. 11.
465 *See id.*, cl. 12.

secure their personal data from their own government. The PDP Bill appears to assume a mature knowledge of the concepts of privacy and consent, which shows a serious lack of care. Even the most educated members of our society are frequently indifferent to these characteristics.[466] Possibly, large scale awareness programmes, especially emphasizing on safety and privacy, could ease the problem and the COVID-19 pandemic has created the appropriate opportunity. Data processors are required to ensure that data principles are informed adequately about the usage of their data. In the health sector, the clinics/hospitals whoever collects the data should have the informed consent of the patients, otherwise, they would be held liable in case of any illegality.

The proposed law bans the processing of sensitive personal data and critical personal data (as defined by the Central Government) outside of India, without specific consent by the data principal and until the Data Protection Authority approves the processing. A non-obstante clause, on the other hand, functions by allowing an individual or agency involved in health or emergency services to explain the need for prompt action.[467] The PDP Bill also prescribes stricter penalties in case of contravention of its provisions.[468] However, experts have expressed concerns about the open-ended exception clauses. They have emphasised that the Bill significantly

---

[466] *See* Padmini Ray Murray and Paul Anthony, *Designing for Democracy: Does the Personal Data Protection Bill 2019 Champion Citizen Rights?*, 55(21) ECO. & POL. WKLY (2020), https://www.epw.in/engage/article/designing-democracy-does-personal-data-protection (last visited May 31, 2021) ("**Murray and Anthony**").
[467] *See id.*, chap. VII.
[468] *See id.*, chap. X.

simplifies the government's task of processing data in order to compulsorily register its residents, blatantly disregarding *Puttaswamy*'s scope, which allows the government to collect data under limited conditions.[469]

Although there is an emphasis on data localization, experts are not convinced. Their contention is based on the assertion that any security and governmental access do not bear any correlation to localisation of the data. In this hyper-connected technological ecosystem, even though the data is stored within the country, the encryption keys can be out of reach of national authorities, unless the data is stored and accessed over a captive private network.[470]

In fact, data localization is a government mandate that data be stored on servers that are physically situated inside a state's borders. It supports the idea of data sovereignty, in which states have the ability to exercise sovereign control over the internet and internet users within their authority.[471] Proponents of data localization say that it is necessary to ensure data privacy. In practice, mandatory data localization might lead to more government surveillance. For a variety of reasons, it compromises privacy. Data localization, for example, compromises information security by increasing the number of data centres that firms must monitor. Furthermore, data localization restricts our service providers to those that

---

[469] *See* Murray and Anthony, *supra* note 466.
[470] *See* Kamal Taneja and Gulshan Rai, *Data Protection Bill is Vague and Intrusive,* HINDU BUSINESS LINE (Mar. 15, 2020), https://www.thehindubusinessline.com/opinion/data-protection-bill-is-vague-and-intrusive/article31075785.ece.
[471] Andrew Keane Woods, *Litigating Data Sovereignty*, 128 YALE L. J. 328, 360 – 63 (2018).

operate locally; experience shows that protectionism affects the quality of a service.[472] Madhulika Srikumar and Bedavyasa Mohanty have accused the Justice B.N. Sreekrishna Committee, mandated to create a national privacy regime, for unconvincingly pushing for data localization. They argue that the Committee's assertation in anticipation of a strong Indian claim in case of accessing of data is a weak one, and dependent on bilateral agreements with entities in countries where our data is stored.[473] However, the same has found its way in the PDP Bill.[474] Stringent procedural norms with regard to providing foreign entities with data is the need of the day. The *Sprinklr case* controversy reminds us that the fears are not completely unfounded.

VI. CONCLUSION

Considering the nature of AI health tools available today, mostly under human supervision, the *res ipsa loquitur* doctrine may lessen the victim's hardship in proving the factum of negligence in case of injuries suffered due to the usage of such tools, yet bigger challenges lie ahead. Due to the inherent nature of opacity in their decision-making, determination of liability among manufacturer, operator or clinician precisely, it is still challenging in many cases. While joint-liability could be a temporary solution, it cannot be a long-term and comprehensive answer. Law would

---

[472] *See* Anupam Chander, *Why Democrats and Republicans Should Oppose Data Localization,* COUNCIL ON FOREIGN RELATIONS (Jul. 20, 2016), https://www.cfr.org/blog/why-democrats-and-republicans-should-oppose-data-localization.

[473] *See* Madhulika Srikumar and Bedavyasa Mohanty, *Data localisation is not enough*, THE HINDU (Aug. 3, 2018), https://www.thehindu.com/opinion/op-ed/data-localisation-is-not-enough/article24584698.ece.

[474] *See* Personal Data Protection Bill, 2019, cl. 37.

require assistance from technology in developing explainable AI which would help the judicial authorities to understand the rationale behind arriving at a specific decision of the tool and then identify where exactly the 'fault' lies.

Further, as witnessed in the Tesla incident, despite the fact that the self-driven cars failed to deliver up to the expectation and gave a false sense of comfort and reliability among the victims, NTSB did not hold Tesla strictly liable for the accidents. The J&J fiasco further illustrates that without stricter approval processes, medical devices have the potential in wreaking havoc.

With an increasing number of AI health tools coming to flood the market in the days ahead, CDSCO must gear up for the challenge of examining and approving AI health devices. The concept of strict product liability is yet to find a niche in our jurisprudence, even if it finds no mention under the new CPA. A legislation or an amendment to the law in this regard would be a welcome move. While dealing with such complicated and potentially dangerous AI tools, owners/clinicians may be mandated to take insurance which may have a compensation cap in case of any injury. However, that would not preclude the right of the patient-victims to approach the civil courts for further compensation. As we continuously strive to improve upon the AI tools that would be able to take more complicated decisions without or with minimal human interference, we would be trekking into the difficult terrains of liability regime. Hence,

incorporating the concept of legal personality for the AI tools appears to be the way forward.

The importance of the protection of personal health data in the AI ecosystem is undeniable, yet in such a vast and diverse country with fragmented networks, effective protection of the data is an uphill task. As the majority of healthcare is in private hands, it is a matter of grave concern as to how the commercial interest of the data processors inside and outside the health sector would eventually play.

Despite the fact that the Personal Data Protection Bill, 2019 has laid emphasis on the consent of data principals, the author holds scepticism over whether the majority of the patients will actually be able to give "informed consent" over their data processing. Further, considering the wide nature of the language used for the processing of personal data envisioned in the PDP Bill under the pretext of dealing with medical emergencies, there is ample scope for data compromise. The *Sprinklr case* only reinstates that scepticism. While we wait in anticipation for the PDP Bill to be signed into law, safeguarding personal health data is to be of paramount significance. The dust is yet to settle.

NLUJ Law Review

Rigved Prasad. K, *Procuring Digital Evidence and the Metaphor Problem: Assessment of India in Comparison to USA, Canada and UK*, 8(1) NLUJ L. REV. 131 (2021).

PROCURING DIGITAL EVIDENCE AND THE METAPHOR PROBLEM: ASSESSMENT OF INDIA IN COMPARISON TO USA, CANADA AND UK

*Rigved Prasad. K**

ABSTRACT

Search and Seizure are a part and parcel of investigations, and the State has legitimate interest in detecting and preventing crimes. Such powers during investigations enable the law enforcement to effectively produce evidence for prosecution and obtain convictions. The development of technology, however, has disrupted this seemingly seamless process of investigation. This is mainly because digital evidence is inherently different from traditional documentary evidence. This fundamental difference demands a deviation from traditional conceptions of privacy and the need to conceptualise new developments such as reasonable expectations of one's anonymity and control of customer information vis-à-vis a third party and many other implications on privacy that digital evidence presents. Instances in which the State could obtain data and the

* The author is a junior associate at BFS Legal, Chennai and may be contacted at **rigvedprasad98@gmail.com**. The author would like to thank their colleague and friend Shrayashree Thiyagarajan, Advocate, Madras High Court, for immensely aiding the author for defining the aim and scope of the paper. The author would also like to extend their gratitude towards Ms. Indumugi C, a final year law student at Tamil Nadu National Law University for their invaluable inputs and insightful suggestions.

criminal procedure applicable would determine whether such intrusion would be reasonable intrusion or not. India's jurisprudence on privacy itself is still in the stage of its infancy. Therefore, it is relevant and necessary to ascertain and analyse how other jurisdictions such as USA, Canada and the UK have conceptualised privacy in light of these new developments and managed to balance the competing rights of an individual and the legitimate state interest. This paper aims to ascertain the effectiveness and the shortcomings of the existing procedure in India to procure digital evidence in comparison to the principles and procedure existing in USA, Canada and UK.

TABLE OF CONTENTS

I. INTRODUCTION

Living in the age of data driven capitalism, it is hard to ignore the enormous amount of information of a person contained in personal electronic devices and remote servers of Internet Service Providers [*hereinafter* "**ISPs**"]. Privacy has to be protected from both State and non-State actors.[475] In corollary, these mammoth repositories of personal information and the constitutional implications of its accessibility to State come into play during criminal investigations.

The absence of data protection law in India has left the right to privacy in a limbo. For instance, while the Supreme Court of India [*hereinafter* "**the Supreme Court**"] required the legislature to put in place a sophisticated legal framework to ensure transparency and accountability of the Aadhaar Scheme;[476] the Aadhaar (Targeted Delivery of Financial and other subsidies) Act, 2016 [*hereinafter* "**Aadhaar Act**"] suffers from major conflicts of interest and excessive delegation, and the Rules thereof appear to be in blatant ignorance of the safeguards suggested in the judgement.[477] Similarly, the infamous Encryption Policy, 2015 that was notified by the Government of India (now withdrawn), mandated every citizen and intermediary to retain an unencrypted message for about 90 days, and

---

[475] *See* Vrinda Bhandari & Renuka Sane, *Protecting citizens from the State post-Puttaswamy: Analysing the Privacy Implications of Justice Srikrishna Committee and the Data Protection Bill, ,* 14(2) SOC-LEG REV. 2018 143, 149-150 (2018); *see also,* K. S. Puttaswamy v. Union of India, (2017) 1 SCC 1, ¶ 328. ("***Privacy Judgement***").

[476] *Id,* 510.

[477] *See generally,* Vrinda Bhandari & Renuka Sane, *A Critique of Aadhaar Legal Framework*, 31 NAT'L L SCH INDIA REV. 22 (2019).

further also mandated intermediaries to share their decryption keys in the garb of licensing, essentially rendering encryption and the use of it inconsequential.[478]

Contrary to popular belief, encryption was not specifically invented to facilitate crime but was only a natural result of the internet transforming from a trust-based community to a non-trust-based platform of communication.[479] Therefore, intermediaries have economic interests in facilitating encryption in their services and devices, and hence resist dilution of encryption.[480] This resistance can also be inferred from Apple Inc. refusing to decrypt an iPhone of an accused when FBI requested it to do so.[481] Right to encryption has also been internationally recognised as a fundamental right due to its ability to provide anonymity to a person in cyberspace.[482] Unfortunately, this facility is also being used for crimes, which the law enforcement terms as the "Going Dark" problem.[483] Therefore, there arises a situation where law enforcement has to depend on

---

[478] Bedavyasa Mohanty, *"Going Dark" in India: The Legal and Security Dimensions in India,* ORF OCCASIONAL PAPER, (Dec. 13, 2016), https://www.orfonline.org/research/going-dark-in-india-the-legal-and-security-dimensions-of-encryption, at 4. ("**Bedavyasa Mohanty**")

[479] Justin (Gus) Hurwitz, *Trust and Online Interaction*, 161 UNIV. OF PENN. L. REV. 1579, 1587 (2019).

[480] Alan Z Rozenshtein, *Surveillance Intermediaries,* 70 STAN L. REV. 99, 122 (2019) ("**Alan Z Rozenshtein**").

[481] *In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, No. 15-MC-1902(JO), 2016 WL 783565 (E.D.N.Y. Feb. 29, 2016) ("**Apple Inc. Warrant**").

[482] Special Rapporteur On The Promotion And Protection Of The Right To Freedom Of Opinion And Expression, UN Doc. A/HRC/29/32 (2015); *see also*, Jeffrey M Skopek, *Reasonable Expectations of Anonymity* 101 VA. L. REV. 691 (2015).

[483] Pratik Prakash Dixit, *Conceptualising Interaction between Cryptography and Law*, 11 NUJS L. REV. 327, 333 (2018). ("**Pratik Prakash Dixit**")

intermediaries, owners of the devices, or the person who possesses decryption key to carry out investigation.

Faced with this legal quagmire, the Supreme Court, has transferred several cases from High Courts across India, and is currently adjudicating upon the legal issue on whether the State can mandate the citizens to link their Aadhar cards to their social media accounts.[484] One of the cases from the Madras High Court involved determining a contentious issue as to whether WhatsApp can be mandated either by the government or judiciary to break the end-to-end encryption offered in its service, in pursuance of facilitating investigation on a case of child pornography.[485] Interestingly, two professors from Indian Institute of Technology, Madras, one of the premiere institutions for technical education in the country, gave contradicting expert evidence regarding whether WhatsApp has the ability to break the encryption.[486] While that question is outside the scope of this paper, this case is a clear demonstration of the government's desperation to use intermediaries for investigation purposes.

Digital evidence is merely evidence in digital form.[487] However, as Lex Gill in his seminal article has elucidated, the normative force of the metaphors used to describe cyberspace and big data and define privacy

---

[484] Facebook Inc. v. Union of India, T.P.(C) No. 1943-1946/2019, decided on 22.10.2019, https://main.sci.gov.in/supremecourt/2019/27178/27178_2019_15_8_17723_Order_22-Oct-2019.pdf.
[485] Facebook Inc. v. Union of India., 2019 (13) SCALE 13, ¶ 7.
[486] *Id.*
[487] Jenia I Turner, *Managing Digital Discovery in Criminal Cases,* 109 J. CRIM. L. & CRIMINOLOGY 237, 244 (2019).

within its contours has adverse legal consequences. The title of this paper borrows the phrase "metaphor problem" to highlight and acknowledge the cognitive gap in our conception of privacy in the digital age or cyberspace in juxtaposition to traditional and physical notions of privacy.[488] In order to demonstrate this, one could imagine a scenario where a police officer forcibly entering a person's house might not find out much about that person's personal life, preferences, habits and the like; in contradistinction, when the police officer searches a smartphone or the data provided by Internet Service Providers, they could obtain both relevant and irrelevant information on almost every aspect of the person's life. Therefore, traditional warrant requirement or warrant specification requirements might be seriously inadequate to protect the privacy of the individual.

Moreover, in a regular search and seizure of a residence the search precedes the evidence, *i.e.*, police sort out relevant and irrelevant objects immediately in the residence and procure the evidence solely required for the purposes of the trial. However, in cases of hard disks, computers or smartphones, the device is initially seized and then searched for evidence by performing cyber forensics.[489] In the process of searching, the irrelevant personal information of the target, or even third parties could be disclosed without the consent of the concerned person. For this reason, the author

---

[488] Lex Gill, *Law, Metaphor, and the Encrypted Machine*, 55(2) OSGOODE HALL L. J. 440, 454 (2018) ("**Lex Gill**").

[489] Paige Bartholomew, *Seize First, Search Later: The Hunt for Digital Evidence*, 30 TOURO L. R. 1027 (2014); *see also,* Swathi Mehta, *Cyber Forensics and Admissibility of Evidence,* PL JAN S-23, S-31 (2012) ("**Swathi Mehta**").

argues that specific warrants to digital locations within a device is necessary in case of digital searches.[490] In the context of procuring evidence from remote servers of third-party intermediaries, the servers contain massive amount of data which are not segregated person-wise thereby posing a greater risk of incidental encroachment into an individual's privacy without his/her consent or knowledge.[491]

In the Supreme Court's *K.S. Puttaswamy and Ors* v. *Union of India and Anr.*verdict [*hereinafter* "***Privacy Judgement***"],[492] the principle of proportionality was adopted, thereby, doing away with the "compelling state interest" test for encroaching into one's privacy. In this context, the substantive and procedural safeguards formed through conceptions of privacy in the physical space, if unquestioningly transposed to the digital space, it would drastically limit the constitutional protection afforded to privacy. Therefore, privacy in the digital space demands more apposite rules and procedural safeguards.[493]

This paper in Chapter II enumerates the different classifications of data that could be used in the course of an investigation. This classification would provide us with a proper understanding of the legal conundrums that digital searches had posed and could pose in the future. Chapter III explains

---

[490] James Saylor, *Computers as Castles: Preventing the Plain View Doctrine from Becoming a Vehicle for Overboard Digital Searches*, 79 FORDHAM L. REV. 2809 (2011).
[491] Sarit K Mizrahi, *The Dangers of Sharing Cloud Storage: The Privacy Violations Suffered by Innocent Cloud Users during the Course of Criminal Investigations in Canada and the United States,* 25 TUL. J. INT'L & COMP. L. 303, 319 (2017) ("**Sarit K Mizrahi**").
[492] *Privacy Judgement, supra* note 475, at ¶ 488.
[493] Orin S Kerr, *Digital Evidence and the New Criminal Procedure,* 105 COLUM. L. REV. 279, 306 (2005) ("**Orin S Kerr**").

the current law that governs the procurement of digital evidence in India emphasising on the overbroad and highly discretionary framework. It also traces the origins and causation of the framework back to the lack of a fundamental right to privacy or reasonable search and seizure. Chapter IV compares and deliberates on the ways in which the United States of America [*hereinafter* "**USA**"], Canada and the United Kingdom [*hereinafter* "**UK**"] have dealt with ensuring protection of privacy in digital search and seizures. This Chapter further attempts to highlight the significance of a constitutionally recognised fundamental right to reasonable search and seizure in these countries, in developing a data protection regime tilted more in favour of their citizens, unlike India. Lastly, Chapter V concludes by inculcating the lessons from the comparative study in the preceding chapters, enumerates vital points on which the framework of digital search and seizure in India needs to be transformed and modified to ensure protection to the citizen's privacy in the real sense.

II. IDENTIFYING CLASSIFICATION IN DATA: STORAGE, CONTENT AND PROTECTION

Understanding classifications in data based on their storage, content and protection would help us better appreciate the procedural and substantive laws that are used to harmonize the conflict between individual privacy and legitimate state interest in detecting crime, as discussed in the following chapters.

A. DATA AT REST AND DATA IN MOTION

Data which is stored in a particular device such as a smartphone, computer, laptop, or hard disk, including data which has been stored in remote servers by service providers are considered to be "data at rest".[494] On the other hand, "data in motion" is when the data in question is in motion or in transmission from one device to another,[495] and if wished to be accessed, it needs to be intercepted, *i.e.*, obstructed from reaching its destination or covertly observe the transmission without the knowledge of the person involved. For example, interception of telephone conversation means eavesdropping on calls, and interception of email communications or even text messages would mean that the message is routed through the police before it reaches the destination.

Here, Kerr explicates this type of classification by making a distinction between "retrospective" and "prospective" surveillance. While the former entails procuring the data or evidence that already exists in the form of digital storage; the latter involves procuring data that would be used for the purpose of investigation which is yet to come into existence.[496] This distinction becomes imperative because prospective surveillance denies the

---

[494] Pratik Prakash Dixit, *supra* note 483, at 332, 333.
[495] *Id.*
[496] Orin S Kerr, *supra* note 493, at 287.

subject of the investigation the "right to delete"[497] and therefore is more invasive.[498]

Unlike traditional services like telephones, it is more difficult to draw the line between prospective and retrospective surveillance in case of messaging services like Instagram and WhatsApp or other cloud service providers. It becomes essential for courts to determine this, since the procedural safeguards and threshold required to issue a warrant, are different for each type of data. Attempts made by courts in the USA and Canada in this regard are progressive and the same are discussed in Chapter IV below.

B. CONTENT AND NON-CONTENT INFORMATION

This classification, as the name suggests, depends on the information that is sought to be procured for the purpose of an investigation. The law enforcement might either need the actual contents of a particular communication, or only the information pertaining to the identity of the sender/receiver or location of the source of the communication.[499] For example, an email address, subscriber information shared with telecommunication providers, an IP address, are all

[497] COUNCIL REGULATION 2016/679 of April 27, 2016, PROTECTION OF NATURAL PERSONS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA, art. 17, 2016 O.L. (L 1191) 1; *see also,* Jorawer Singh Mundy v. Union of India, 2021 SCC OnLine Del 2306 (India).
[498] Patricia L Bellia, *The Memory Gap in Surveillance Law*, 75 U CHI. L. REV. 137, 161-166 (2008) at 176.
[499] Swathi Mehta, *supra* note 489, at ¶ 31.

characterized as "non-content information."[500] However, the actual contents of a telephone call, a text message or the body of an e-mail sent from one person to another, is considered to be "content information".[501] This kind of distinction seems to be relevant when law enforcement approaches third parties for information on their customers, instead of directly conducting a search and seizure of the subject of the investigation. Clearly, when law enforcement authorities could directly seek and obtain content-information from third parties, it is more intrusive than when non-content information is sought for.

Even procedural safeguards in obtaining the same would differ, for example while non-content information could be procured from third party without the consent of the end customer, or it could even be argued that such consent need not be obtained, but the same could not be the case for contents of particular communications of the customer.[502] This distinction further grants the warrant granting authority an opportunity to minimise the data that is to be procured by the law enforcement.[503]

---

[500] Mathew J. Tokson, *The Content/Envelope Distinction in Internet Law,* 50.6 Will. & Mary L. Rev. 2105, 2113-2116 (2009).
[501] Orin S Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN L. R. 1005, 1019 (2010).
[502] Dan Jerker & Lodewijk Van Zweisston, *Law Enforcement Access to Evidence via Direct Contact with Cloud Providers- identifying the Contours of a Solution,* 32 COMP. L. & SEC. REV. 671, 679 (2016).
[503] *Id.*

C. ENCRYPTED DATA

Given that a lot of personal information is stored in devices and remote servers, and further considering the prominence of social media in today's world, any consumer would wish to protect their personal information. Encryption offers that protection by transforming plaintext into unintelligible form either by way of one-way (impossible to recover) or two-way encryption.[504] The purpose of it is to make the data unreadable to anyone other than the person who has the decryption key.[505]

Generally, arguments against encryption or for diluting encryption presuppose a privacy-security trade-off,[506] where the privacy of an individual is sacrificed for the security of another/ the greater good. However, it is a bit parochial to suggest that encryption disregards security interests since encryption offers protection to the data of any person available in any electronic device/storage device. Therefore, the contradictions of encryption and security are better understood only as a security-security trade-off, *i.e.*, the security of one individual is compromised for the security of another.[507] This is precisely the reason why the Encryption Policy, 2015, that was proposed by the Indian government (now withdrawn) and provided for overreaching investigatory powers to the state, prohibitive data retention requirements and also for a centralised

---

[504] Information Technology (Certifying Authorities) Rules, 2000, Schedule V.
[505] Orin S Kerr & Bruce Schneier, *Encryption Workarounds,* 106 GEO L. J. 989, 994 (2018) ("**Kerr & Schneier**").
[506] Alan Z Rozenshtein, *supra* note 480, at 137
[507] *Id.*

decryption key in control of the government,[508] was vehemently opposed by the intermediaries and general public.

There are broadly two types of encryptions currently used by service providers. The first type is where the encryption key cannot directly be used by the consumers such as in services like email, ATM machines, smartphones or other devices. [509] The end user of the product or service is likely to create a password or a passcode which in turn decrypts the decryption key in the first instance, followed by the key decrypting the content.[510] This could be further classified into symmetric and asymmetric encryption. This distinction, however, is not necessary since symmetric encryption is outdated, and currently due to the advantages in its application, only asymmetric encryption is used in almost all e-commerce and internet services.[511] Asymmetric encryption entails a "public key known to all persons" and a "private key" which is only used by recipient to decrypt the messages, essentially enabling random but secure transactions and interactions in cyberspace.[512]

The second type of encryption can be seen in services that employ end-to-end encryption, wherein the process of decryption is "practically invisible to the consumer".[513] This kind of encryption has gained a lot of

---

[508] Bedavyasa Mohanty, *supra* note 478, at 4 -7.
[509] Pratik Prakash Dixit, *supra* note 483, at 330.
[510] *Id.*
[511] *Id.* at 331.
[512] *Id.*
[513] Kerr & Schneier, *supra* note 505.

traction in messaging services such as WhatsApp, Signal and Telegram. The primary goal of end-to-end encryption is to ensure the consumers their privacy and sometimes particularly anonymity.[514] Unlike asymmetric encryption, in the case of end-to-end encryption, even the service provider do not possess the keys required to decrypt content, which makes it practically impossible for them to provide the key to a government agency.

Encryption techniques leave the law enforcement's hands tied. This means that they need to depend either on the owner of the personal devices or third-party intermediaries for passwords/decryption. In the former, the right against self-incrimination[515] is triggered when the police or courts are trying to obtain the data by forcing the accused/owner of the personal device to provide the password. The latter gives rise to a host of issues ranging from, the extent to which a third-party intermediary is required to divulge personal information of the customer to the procedural safeguards for law enforcement to obtain encrypted information.

III. INDIAN LAW ON PROCURING DIGITAL EVIDENCE

There are very few judgements discussing the direct conflict between search and seizure and an individual's right to privacy in India. The Supreme Court in *M. P. Sharma v. Satish Chandra*[516] had defined search and seizure as an "overriding right" of the State in the interest of security. In the Supreme Court's opinion, restricting security interests by reading in

[514] Alan Z Rozenshtein, *supra* note 480, at 137.
[515] INDIA CONST., art. 20 cl. 3.
[516] M. P. Sharma v. Satish Chandra, AIR 1954 SC 300 ("***M. P. Sharma***").

right to privacy would be contrary to the intention of the framers of the Constitution of India [*hereinafter* "**the Constitution**"], specifically emphasizing that our Constitution lacks provisions similar to 4th Amendment in the USA or Section 8 in the Charter of Bill of Rights in Canada.[517] Only much later in *Gobind v. State of Madhya Pradesh*[518] did the Supreme Court indicate that a "compelling state interest" can legitimately encroach upon a person's fundamental right to privacy (recognised under Article 21 of the Constitution). Except for recognizing that detecting crime is a legitimate state interest,[519] the Supreme Court in overruling *Gobind v. State of Madhya Pradesh* in the *Privacy Judgement* had not dealt with the contradictions between an individual's right to privacy, and the scope of the law enforcement's power in case of a search or seizure. Clearly, the privacy jurisprudence in India is in its nascent stages. No attempt has been made by the legislature to reconsider the existing provisions for search and seizure, and the surveillance power of government in the light of the *Privacy Judgement*.

A. DATA AT REST

The provisions of the Criminal Procedural Code, 1973 [*hereinafter* "**CrPC**"] in respect of search and seizure appears to be the only law applicable in respect of procurement of data at rest.[520] According to this law, for any 'place' to be searched a general search warrant is required.[521]

---

[517] *Id.* at ¶ 20.
[518] Gobind v. State of Madhya Pradesh, 2 SCC 148 (1975), ¶¶ 24,28.
[519] *Privacy Judgement, supra* note 475, at 484.
[520] CODE CRIM. PROC., §93.
[521] *Id.*

The warrant shall be granted if the Magistrate "has reason to believe" that it is necessary for investigation or trial. However, there are no specific additional requirements prescribed for a police officer to minimize the scope of the search, if such search is undertaken on an electronic device. Though, the Magistrate has the discretion to add more specifications to the warrant restricting the scope of the search, there have been no cases where it has been used for electronic devices.[522]

In India, the police have a large scope to circumvent these warrant requirements as they have the powers to obtain the device without judicial oversight. The police also have the discretion to issue a written order mandating a person to produce a document or a thing.[523] There is also no burden on the police officer or the magistrate issuing summons to adjudicate, or pass the muster of a probable cause or a reasonable ground threshold; the written order can be issued solely on the basis of whether the officer feels it is "necessary or desirable".[524] The police officer has the discretion to search any place in his jurisdiction without a warrant and all that the officer needs for justifying the same is merely his "opinion" that such procedure would cause "undue delay" in the investigation.[525] This insubstantial framework is further devitalised by the courts in India which have also rejected the "fruit of the poisoned tree" doctrine[526] (which renders

[522] CODE CRIM. PROC., §93(2).
[523] CODE CRIM. PROC., §91.
[524] *Id.*
[525] CODE CRIM. PROC., §165.
[526] Silverthorne Lumber Co. v. United States, 251 U.S. 385 (1920).

any evidence to be inadmissible in court, if it has been obtained by illegal means, not following due process of law), and has held that the evidence collected without the authority of law is not illegal or inadmissible in court of law but merely a procedural irregularity.[527]

The Information Technology Act, 2000 [*hereinafter* "**IT Act**"] applies where data has to be obtained from ISPs or social media service providers. The primary objective of the IT Act was to legitimise the use of digital signatures and also provide a comprehensive framework to preserve its authenticity.[528] Unless in circumstances provided under the Act or any other law, an intermediary is prohibited from disclosing any person's personal information.[529] However, the IT Act does not have a provision which explicitly authorises a government agency or police officer to collect information from a third party.

The safe harbour provision of the IT Act which exempts intermediaries from liability mentions that the intermediary is bound to observe "due diligence" or any other guidelines as prescribed by the Central Government.[530] The due diligence required by the Central Government does not provide for any *ex ante* judicial supervision on the process of procuring data from intermediaries, but mandates that the intermediary

---

[527] Pooran Mal v. Director of Inspection AIR 1974 SC 348, ¶ 34; *see also,* State of Maharashtra v. Natwarlal Damodardas Soni, AIR 1980 SC 593, ¶ 9; Radhakrishnan v. State of UP, 1963 Supp. 1 S.C.R. 408.
[528] Shruti Chaganti, *Information Technology Act: Danger of Violation of Civil Rights*, 38 EPW WEEKLY 3587-3595 (August 23-29, 2003).
[529] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, § 72A.
[530] *Id.* at §79(c).

shall provide the data within 72 hours of an order in writing, stating the reasons for such a request by a *"Government agency lawfully authorised for investigative or protective or cyber security activities"*.[531] Intermediaries also comply with such requests to prevent any unnecessary liability because assistance in such a manner is not regarded as an invasion to privacy in this legal framework, but a form of due diligence that the intermediary is bound to follow to prevent any kind of penalty.[532]

The encryption of personal devices poses yet another conundrum. In this case, the law enforcement needs to depend on the subject of the investigation to procure the data itself. If the personal devices are locked due to encryption by the subject, then there is a possibility that the law enforcement will force the subject to provide the password. In case, the devices are locked using a finger print, the bar under Article 20(3) of the Constitution will not operate because the Supreme Court in *State of Bombay v. Kathi Kalu Oghad* [*hereinafter "**Kathi Kalu**"*] held that finger prints, retinas, handwriting or signature samples even though amount to furnishing evidence, concealing the same cannot "change its intrinsic character" and therefore will not amount to "being a witness" against himself.[533] The concurring judgement of Justice Das Gupta (speaking for Justices Sarkar and S.K. Das) took a contrary view of the phrase "to be a witness" in Article 20(3) and held that it includes providing documentary evidence under

---

[531] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r.3(j).
[532] *Id.* r.7.
[533] State of Bombay v. Kathi Kalu Oghad, AIR 1961 SC 1808, ¶ 12 ("***Kathi Kalu***").

compulsion, whereas the majority judgement of Chief Justice B.P. Sinha specifically excluded them and restricted the scope only to furnishing testimonial evidence.[534]

There has been a considerable shift in interpreting the right against self-incrimination. While *Kathi Kalu* relied heavily on the nature of evidence, *Selvi v. State of Karnataka*[535] [*hereinafter* "***Selvi***"] seems to have placed more emphasis on the personal autonomy and right of the accused/subject to reveal his information.[536] It was held in *Selvi* that Article 21 and 20(3) of the Constitution are interrelated and essentially conceptualised self-incrimination in terms of personal autonomy and control that a subject has over what information they could divulge during an investigation.[537] However, its applicability to data within personal gadgets already confiscated is questionable because the Supreme Court was only dealing with whether the evidence in question is testimonial or material in nature.[538] Digital evidence falls under "documentary" evidence,[539] and the same is outside the scope of Article 20(3) unless the document in question is a confession obtained through coercion as per the ratio of *Kathi Kalu*.[540] Furthermore, it is interesting to note that even though the opinion of Justice

---

[534] *Id.* at ¶ 13.
[535] Selvi v. State of Karnataka, AIR 2010 SC 1974 ("***Selvi***").
[536] *See generally,* Aditya Sarmah, *Privacy and Right against Self-incrimination: Theorising a criminal process in the Context of Personal Gadgets*, 3 CONST. AND ADMIN. L. QUAT. 30 (2017) ("**Aditya Sarmah**").
[537] *Selvi*, *supra* note 535, at ¶ 191-193.
[538] *Id.* at ¶ 129.
[539] Evidence Act, 1872, §3.
[540] *Kathi Kalu*, *supra* note 532.

Das Gupta in *Kathi Kalu* held that the words "to be a witness" included documentary evidence,[541] it managed to concur with the majority. Justice Das Gupta, interpreting the words 'against himself', held that since providing his fingerprint was only for the purpose of comparison with the document already in possession of the police, it would not amount to self-incrimination as he is not directly providing evidence against himself.[542] Following *Kathi Kalu* and *Privacy Judgement*, the Karnataka High Court very recently issued guidelines for procuring electronic evidence which specifically states that forcing a witness to provide password or fingerprint is not barred by Article 20(3) and that the investigation officer is within his power to require a citizen or an intermediary to decrypt any information.[543]

B. DATA IN MOTION

It is important to understand the development of the interception of "telegraphic communications"[544] in order to critically examine the current provisions pertaining to interception of electronic communications under the IT Act. The limitations placed for the purpose of interception of telegraphic communications was based on restrictions to free speech from Article 19(2) of the Constitution (excluding defamation).[545] This clearly defines the purpose for which such interception shall be made and the same was also subject to judicial review (this review is only *ex post* surveillance),

---

[541] *Id.* at ¶ 27-33.
[542] *Id.* at ¶ 36-37.
[543] Virendra Khanna v. State of Karnataka, MANU/KA/0728/2021, ¶ 12.25, 12.26 & 15.
[544] The Telegraph Act, 1885, § 3(1).
[545] Bedavyasa Mohanty, *Inside the machine Constitutionality of India's surveillance apparatus*, 12 IND. JOUR. LT 206, 212 (2016).

unlike the previous version where interception is justified by proving "public emergency" or "public safety", the existence of which is to be wholly determined by the Executive.[546]

While almost replicating the provision in the Telegraph Act, the additional words "for any other investigation"[547] in the IT Act enables any agency authorised by state or Central government, or officers authorised by either of them, to intercept electronic communications for any purpose. The intermediaries would face criminal charges if technical assistance or any other facilities under Section 69(3) of the IT Act is not provided.[548] This deviation from the purpose limitation that exists in the Telegraph Act is completely unfounded and unsubstantiated.

Moreover, scope of "assistance" by an intermediary is very vaguely worded and could encompass all types of assistance including decrypting content information for the purpose of investigation without the knowledge of the customer. The assistance requirement not only includes interception, but also extends to decryption and the intermediary is exempted from the criminal liability only when it is practically impossible for them to decrypt it.[549] It is to be noted that decryption orders under the said rules extends to both, data in rest and data in motion.

---

[546] *Id.*
[547] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, §69.
[548] *Id.* at §69(4).
[549] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, r.17 ("**Interception Rules**").

It is clearly noticeable that there is absolutely no attempt by the legislature to classify data as elaborated in Chapter II, to specifically provide procedures for each of them. On the contrary, the provision enabling interception, monitoring and decryption is merely a blanket power in the hands of police. The procedural safeguards that are notified by the Central government[550] do not provide for any warrant or prior judicial authorisation for the police to intercept electronic communications.[551] The entire process from the grant of approval[552] to the periodic review of the approvals[553] rests with the executive.

The procedural safeguards in the IT Act for interception was also a mere replication of the guidelines issued in the case of *People's Union for Civil Liberties (PUCL)* v. *Union of India* [*hereinafter* "***PUCL***"].[554] While the powers to intercept telegraphic communications was challenged, the Supreme Court formulated guidelines in *PUCL*[555] which was later codified in the Telegraph Rules.[556] In framing the guidelines the Supreme Court specifically refrained from providing for a prior judicial authorisation since it would not be within the scope of the principal legislation.[557] In merely replicating these guidelines and also diluting the purpose limitation existing in the

---

[550] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, §69.
[551] Interception Rules, *supra* note 531, at r.3.
[552] *Id.*
[553] *Id.* at r. 2(q)
[554] *See Generally*, Vishal Kanade, *Tap-Tap Who is Listening-Prying into Privacy*, 5 L. REV. GLC 171 (2006).
[555] People's Union for Civil Liberties v. Union of India, 1 SCC 301 (1997) ("***PUCL***")
[556] The Telegraph Rules, 1951, r.419A.
[557] *PUCL*, *supra* note 555, at ¶ 34.

Telegraph Act, the legislature has significantly reduced the scope of protection to its privacy. The principles and procedures propounded in *PUCL* are also very outdated and even though it is in the context of mass surveillance, in light of recent developments in technology and the privacy jurisprudence in India, it needs to be revisited.[558] These procedures currently lack any mandate as to interception/intrusion into one's privacy being the least restrictive measure among other possibilities, lacks any specific tailored procedures for each type of data, are over broad provisions and does not take into account the severity of the offence. It is apparent that the Telegraph Rules do not pass the muster of proportionality test as propounded in the *Privacy Judgement*. Currently, more than ten agencies are authorised by the Central government to demand information of any kind on citizens that is in possession of third-party intermediaries.[559]

India has always preferred the "Crime Control Model" over the "Due Process Model", placing more emphasis on "eliminating crime" than individual liberties of the accused.[560] It can be gleaned from the legal framework for procuring digital evidence in India that there is no effort to balance the competing interests of the State and the individual. There is no law legitimising the power of law enforcement to mandate information from third party service providers, but the power itself is defined in terms

---

[558] Chaitanya Ramachandran, *PUCL v. Union of India Revisited: Why India's Surveillance Law must be Redesigned for the Digital Age,* 7 NUJS L. Rev. 105 (2014).
[559] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, § 69; Ministry of Home Affairs, Order S.O. 6227(E) dated December 20, 2018, http://egazette.nic.in /WriteReadData/2018/194066.pdf.
[560] Aditya Sarmah, *supra* note 536, at 39.

of obligations that the intermediaries are bound to follow to prevent getting wounded up in any criminal proceedings instituted against them. The Intermediary Guidelines place further burden on the intermediaries such as mandating them to enable tracing of individuals[561] and also require them to proactively determine and remove unlawful content,[562] which in essence amounts to privatising law enforcement.

IV. PROCURING DIGITAL EVIDENCE IN OTHER JURISDICTIONS

This chapter looks at the negative obligation of the state not to intrude into an individual's privacy, as it exists in the USA, Canada and the UK in terms of digital evidence. These countries were chosen as they were extensively discussed in the *Privacy Judgement* while recognising informational privacy. This comparison is done solely for the purpose of understanding the intricacies and predicaments that the courts have struggled with and also how the "metaphor problem" has been addressed or overcome in these jurisdictions. Even though, these regimes are not ideal and are still evolving, in juxtaposition to India they appear to be much more mature in terms of procedural due process.

A. UNITED STATES OF AMERICA

The framework developed in USA can be characterized as a patchy work, developed sporadically over a period of time, as and when the digital

[561] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 3(j).
[562] *Id.,* r. 4(4).

market demanded such laws, and is often criticised for the same reason.[563] Procurement of digital evidence is considered to be a Fourth Amendment Search under the US Constitution and therefore all the principles of reasonable search and seizure apply automatically.[564] Given the high regard for privacy rights given in the USA post-independence, it seems incredibly difficult to translate them into the context of digital evidence[565] and in that process, some compromises have been made.

i. Warrant, but Only for 180 Days

The Stored Communications Act, 1986, distinguishes between an Electronic Communication Service [*hereinafter* "**ECS**"] provider and a Remote Computing Service [*hereinafter* "**RCS**"] provider, for the purpose of allowing any government entity to procure data from a third party.[566] While the former can be messaging services like WhatsApp, Facebook Messenger or email services, the latter comprises of services provided only for the purpose of storage "on behalf" of the consumer.[567] The ECS and RCS providers aren't mutually exclusive and most of the times the services overlap. For example, social media websites provide communication services and also act as RCS providers.[568] It is pertinent to note that unlike

---

563 Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, Fourth Amendment, and Statutory Law Enforcement Exemptions,* 111 MICH. L. R. 485, 495 (2013).
564 Orin S Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 564 (2005) ("**Kerr**").
565 *See generally,* Donald A Dripps, *Dearest Property: Digital Evidence and the History of Private Papers as Special Objects of Search and Seizure,* 103 J. CRIM. L. & CRIMINOLOGY 49 (2013).
566 18 U.S.C §2703 (1976).
567 *Id.* at § 2711(2).
568 Crispin v. Christian Audigier, Inc. 717 F. Supp. 2d 965 (C.D. Cal. 2010).

the classifications mentioned in Chapter II, this distinguishes between the types of service that a third party provides the user.

Apart from defining ECS in terms of type of service, the Act prescribes an arbitrary cut-off date of 180 days, within which the government is mandated to get a warrant from a court of competent jurisdiction to procure data from ECS providers.[569] However, after 180 days, the law deems that the storage of such communication is not for providing any communication services such as emails or messages, but the service provider only acts as an entity providing storage for the user. Hence, after 180 days, a subpoena, as applicable to an RCS provider, is enough to mandate the intermediary to provide the content information provided prior notice is given to the consumer.[570] If the government entity doesn't want to provide notice it has to either opt for a warrant[571] or a get judicial authorisation for a delayed notice.[572]

This warrant requirement flows from the Fourth Amendment, which mandates that for the citizen shall not be subject to "unreasonable search and seizure" and therefore the judge would have to be satisfied that there is "probable cause" for a warrant to be granted.[573] Usually, the law

---

[569] 18 U.S.C §2703(a) (1976).
[570] *Id.* at 2703(b).
[571] *Id.*
[572] 18 U.S.C §2705 (1976).
[573] Reema Shah, *Law Enforcement and Data Privacy: A forward Looking Approach,* 125 YALE L. J. 543, 545 (2015).

enforcement waits for 180 days since the RCS requirements are relatively less stringent than the ECS requirements.[574]

Furthermore, the lower courts have also distinguished between opened and unopened communications stating the reason that when a message or email is opened within 180 days, then the ECS provisions ceases to apply because once the communication has reached the destination, the service provider only stores the same on behalf of the consumer and therefore acts as an RCS provider.[575] The Supreme Court of the United States [*hereinafter* "**SCOTUS**"] also emphasised the differential expectation of a citizen's privacy in case of content and non-content information.[576] Any non-content information from an ECS or an RCS provider can also be done only through a court order.[577] Even though the 180 days cut-off seems arbitrary, the mandatory warrant requirement and the explicit consent requirement, seems to provide sufficient judicial oversight prior to procuring the personal data.

ii. Acknowledgment of the Metaphor Problem by the Judiciary

The US jurisprudence had formulated the "third party" doctrine, which negates the existence of a reasonable expectation of privacy if

---

[574] Sarit K Mizrahi, *supra* note 491*,* at 333.
[575] Christopher J. Borchet et al., *Reasonable Expectations of Privacy Settings: Social Media and the Stored Communications Act,* 13 DUKE L. & TECH REV. 36, 49 (2015).
[576] Sarah Wilson, *Compelling Passwords from Third Parties: Why the Fourth and Fifth Amendments Do Not Adequately Protect Individuals when Third Parties Are Forced to Hand Over Passwords*, 30 BERKLEY TECH. L. J. 1, 17(2015) ("**Sarah Wilson**").
[577] 18 U.S.C §2703(c) (1976).

information is voluntarily disclosed to a third party.[578] Contrary to that, in cases of cell phones 'cell site location data", the SCOTUS held that in this digital age all data shared to intermediaries could not possibly be a voluntary affirmative action on part of the customer that negates the legitimate expectation of privacy.[579] In yet another instance, the SCOTUS held that compelling production of emails from ISPs without warrant is unconstitutional irrespective of it being a third party.[580] Similar to this departure from the third party doctrine, the SCOTUS in the context of frisking and searching a person, held that unlike normal documents of a person, a cell phone differs *"qualitatively and quantitatively"* and has the potential to disclose almost every personal information of any citizen and therefore, a warrant is required for searching the same.[581]

The Federal Rules of Criminal Procedure also recognise the two-step process involving seizing and searching of personal devices and data storage devices and allows copying of data on site.[582] The results of this overt emphasis on the metaphor problem by the SCOTUS is clearly reflected in the recent trend of magistrates across the USA including minimisation requirements in their warrants, essentially issuing protocols providing for minimal and only necessary data to be accessed to ensure that

[578] Katz v. United States, 389 US 347 (1967).
[579] Carpenter v. United States 138 S.Ct. 2206 (2018), ¶ 18-22.
[580] United States v. Warshak, 631 F.3d 266 (6th Cir. 2010)
[581] Riley v. California, 573 U.S.373 (2014), ¶ 17-21.
[582] Fed. R. Crim. P. 45(a)(e)(2).

the informational privacy of their citizens is protected.[583] Even though it is not considered a constitutional requirement,[584] the warrant for search of an electronic device was accompanied with protocols to restrict the data that is procured; for example, a mandatory condition restricting the search to data with ".jpg" (picture) file extension.[585] Clearly, with lack of any guidance and affirmative pronouncement of the Indian judiciary on the metaphor problem, unlike USA, the lower courts in India find absolutely no use for minimisation requirements.

iii. The Hurdles Surrounding Interception

While the Wiretap Act[586] regulated the process of intercepting telephone communications, the Electronic Communications Privacy Act, 1986[587] amended these provisions to make them compatible with electronic communications.[588] In case of interception of electronic communications, a prior authorisation of the application must be granted by the Attorney General in case of an application to a Federal Court judge, and principal prosecuting attorney in case of a State Court judge.[589] The offences for which an authorisation could be provided, is exhaustively enlisted in the legislation which means that the purpose for which law enforcement could

---

583 *See Generally,* Emily Berman, *Digital Searches, the Fourth Amendment, and the Magistrates 'Revolt',* 68 EMORY L J 82(2018).
584 *United States v. Comprehensive Drug Testing, Inc.,* 513 F.3d 1085 (9th Cir. 2008).
585 *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999).
586 Title III, Omnibus Crime Control and Safe Streets Act, 1968 (Wiretap Act).
587 18 U.S.C §2510-2522 (1976).
588 Sarah Wilson, *supra* note 102, at 31.
589 18 U.S.C §2516 (1976).

invoke this power is restricted.[590] The court must be satisfied of probable cause of the offence itself and the probable cause of the interception providing evidence. Furthermore, the court must also be satisfied of the complete exhaustion of other investigative methods or confirm that they "reasonably appear unlikely to succeed".[591] A judge of competent jurisdiction, in case of interception does not include magistrates unless the statute specifically provides for the same, but only includes a district or court of appeals judge.[592]

Communications Assistance for Law Enforcement Act, 1994 [*hereinafter* "**CALEA**"] is primarily a law mandating assistance to law enforcement for the purpose of wiretapping and it applies only to "telecommunications carriers".[593] Compliance with substantive provisions in CALEA would be necessary for facilitating a wiretap, and as a consequence the judge passing the court order is also given the power to enforce the same.[594] However, contrary to popular belief these provisions do not apply to electronic communication services and do not address encryption in any manner.[595] The Federal Communications Committee [*hereinafter* "**FCC**"], is given the power to expand the scope of the CALEA and deem any service that replaces the local telephone exchange services as

---

[590] *Id.*
[591] *Id.* at 2518(3).
[592] *Id.* at 2510(9).
[593] Justin (Gus) Hurwitz, *Encryption Congress Mod (Apple + CALEA),* 30 HARV. J. L. & TECH. 355, 376 (2016) [*hereinafter*, "**Justin (Gus) Hurwitz**").
[594] 18 U.S.C §.2522 (1976).
[595] Justin (Gus) Hurwitz*, supra* note 593, at 382.

a "telecommunication carrier", but there is still an ambiguity as to whether it could apply to WhatsApp and email services which primarily provide the specifically exempted "information services" under the CALEA.[596] This differential approach towards "interception" is because it is more intrusive than procuring data at rest. Not only prior judicial authorisation in terms of warrant is required, but a District or Appeals Judge is required to be satisfied that interception is the last possible tactic to procure information and prosecute the offenders.[597]

iv. Encryption and the Silent Spectator

With respect to encryption, the legal framework in the USA remains silent. While it authorises government entities to procure data from third parties, there is no mandatory requirement for the third party to provide the decryption key. While the FBI cited that the courts still had the power to mandate the intermediary, in a case involving Apple Inc. under the All Writs Act,[598] the Court rejected the argument and held it had no obligation to decrypt the phone.[599] While in the late 1990s it was argued that courts were not very keen on including rights beyond the text of the US Constitution,[600] clearly courts now have realised that due process requirements under the Constitution need to be self-tailored to adapt to the new implications of digital evidence on the right of privacy. However, the

---

596 *Id.* at 387.
597 18 U.S.C § 2518(3)(c) (1976).
598 28 U.S.C § 1651 (2012).
599 Apple Inc. Warrant, *supra* note 481.
600 *See Generally,* Zhonette M Vedder-Brown, *Government Regulation of Encryption: The Entry of Big Brother or the Status Quo* 35 AM. CRIM. L. REV. 1387(1998).

protection offered by a mandatory key disclosure law, if passed, would heavily depend upon the kind of metaphor that the courts choose to apply to an encrypted information.[601]

The police could also compel the owner of a personal gadget to decrypt a message. In case of providing a fingerprint, just like *Kathi Kalu* in India, the courts in USA could justify the same by citing *State v. Doe*[602] which came to a similar conclusion, *i.e.*, compelling to produce fingerprints wouldn't amount to incrimination and is not hit by the Fifth Amendment. While compelling to produce documentary evidence including digital evidence, does not necessarily attract the Fifth Amendment, unlike India, the US courts have developed an exception called the act-of-production testimony, *i.e.*, the act of producing the document by itself is testimonial in nature and incriminates the citizen.[603] Interestingly the exception to that application is the presence of a foregone conclusion which means that the police were already aware of this knowledge or the contents of the documents, and in that case it would not be deemed testimonial.[604] *Commonwealth v. Dennis Jones*[605] is the only case that clearly sets out the law on compelling decryption of personal devices, and the Court held that the Fifth Amendment protection extends only to testimonial acts, and the law

---

[601] A Michael Froomkin, *Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution,* 143 U PA L. REV. 709, 884 (1995).
[602] State v. Doe, 465 U.S 605.
[603] Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices,* 87 FORDHAM L. REV. 203, 219 (2018).
[604] *Id.*
[605] Commonwealth v. Dennis Jones, 117 N.E.3d 702 (Mass. 2019).

enforcement can compel a person to provide their password if it is proved "beyond reasonable doubt" that the defendant knows the password.[606] However, it is unclear as to how the subject's right against self-incrimination and forced testimony could be influenced by his knowledge of the device's password.

B. CANADA

Similar to the Fourth Amendment to the US Constitution, Section 8 of the Charter of Rights of Canada,[607] protects citizens from unreasonable search and seizure. The Supreme Court of Canada [*hereinafter* "**Canadian SC**"] laid down the pre-requisites for a valid search namely pre-authorisation by a neutral body,[608] authorised by a reasonable law and reasonableness in the search itself.[609] A reasonable expectation of privacy is a prerequisite for a particular search to fall under Section 8, and consequentially such search to be subject to various constitutionally guaranteed procedural and substantive safeguards.[610] The provisions regarding procuring digital evidence are encapsulated in the Criminal Procedure Code of Canada.

---

606 David Rassoul Rangaviz, *Compelled Decryption & State Constitutional Protection against Self-Incrimination,* 57 AM. CRIM. L. REV. 157,158 (2020).
607 Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, being Schedule B to the Canada Act, 1982 (U.K), 1982, c. 11.
608 Hunter v. Southham, [1984] 2 S.C.R 145.
609 Lee Ann Conrod, *Smart Devices in Criminal Investigations: How Section 8 of the Canadian Charter of Rights and Freedoms Can Better Protect Privacy in the Search of Technology and Seizure of Information,* 54 APPEAL 115, 121(2019) ("**Lee**").
610 *Id.*

i. Data at Rest: Subjective Judiciary and an Equivocal Parliament

The general search warrant[611] is the most commonly used provision to seize and search devices, and storage drives of the subject. In the context of a general search warrant as regards personal electronic devices like computers or laptops, the Canadian SC[612] rightly addressed the metaphor problem. It held that receptacles as understood previously cannot be applied to these devices, and specific prior judicial authorisation was absolutely necessary to seize and search these devices.[613] While warrantless searches are usually allowed in case of search incident to arrest, the Canadian SC[614] held that personal devices such as smartphones are capable of having varying degrees of personal information and hence could not be equated to a purse or a briefcase.[615] However, in both the cases a specific protocol to search or a minimisation requirement within the warrant was not considered constitutionally necessary.[616] Furthermore, the Canadian SC also specifically refrained from formulating particular tests and also pinning the level of protection offered to a citizen to the level of protection offered by technology itself.[617] For example, it cannot be argued that merely because

---

611 Criminal Code, R.S.C, (1985) c. C-46, §487.01 ("**Criminal Code**").
612 R v. Vu, [2013] 3 SCR 657.
613 *Id.* at ¶¶ 49,50.
614 R v. Fearon [2014] SCR 621.
615 *Id.* at ¶¶ 180-183.
616 Susan Magotiaux, *Out of Sync: Section 8 and Technological Advancement in Supreme Court Jurisprudence,* 71 SC L. REV.: OSGOODES ANN. CONST. CC 501, 508 (2015) ("**Susan**").
617 *Id.*

a citizen does not have an encryption to his smartphone there exists no reasonable expectation to privacy.

In case of procuring data from third parties like ISPs and Online Content Service [*hereinafter* "**OCS**"] providers, the framework consists of different types of production orders namely general production order,[618] production of transmission data,[619] tracing a particular communication,[620] tracking data[621] and even financial data.[622] The judge deciding a case, would have to be satisfied that such data would aid in the investigation of any offence.[623] Similar to the USA, information as to identity or non-content information are considered to be outside the scope of privacy.[624] This is also reflected in the different thresholds specified, such as "reasonable grounds to believe" for a general production order, and "reasonable grounds to suspect" for orders involving transmission of data, or specific communications.

The Canadian SC, emphasising on anonymity, has recently held that even basic subscriber information collected from ISPs are of a nature that it could reveal the intrinsically personal information which the subscriber wishes to keep a secret or remain anonymous, and the same would be

---

618 Criminal Code, R.S.C, (1985) c. C-46, §487.014.
619 *Id.*, at §487.016.
620 *Id.*, at §487.015.
621 *Id.*, at §487.017.
622 *Id.*, at §487.018.
623 *Id.*, at §487.015.
624 R v. Plant, [1993] 3 S.C.R 281; *See* R v. Spencer, (n.127).

reasonable only if there is prior judicial authorisation.[625] The Canadian SC has also acknowledged that a person could have reasonable expectation of privacy over a text message sent by him/her, stored in the device of some other person.[626] The courts have consistently refrained from formulating any rigid tests, and prefer to decide them on a case to case basis, probably to prevent the derailment of an evolving privacy jurisprudence.[627] However, in spite of rejecting the third-party doctrine, the courts have found a way to circumvent the lack of access to the data by including the contracts between the service providers and customers as an important criterion to decide whether there is a reasonable expectation of privacy.[628]

In pursuance of a conscious effort to retain the flexibility of Section 8 jurisprudence, courts in Canada have formulated several caveats[629] that have resulted in ambiguity in applying the law. Additionally, the Criminal Procedure Code of Canada also exempts every entity from any kind of liability as to voluntarily disclosing information to the law enforcement for the purpose of an investigation without the consent of the service provider.[630] This obliqueness has provided enough ambiguity and leeway for the law enforcement to circumvent warrants and obtain data from third parties to aid their investigations.[631] Even recently, Protecting Canadians

[625] R v. Spencer, 2014 SCC 43, ¶¶ 38, 68.
[626] R v. Marakah, 2017 SCC 59.
[627] Lee, *supra* note 609, at 115-117.
[628] Sarit K Mizrahi, *supra* note 491, at 328.
[629] Lee, *supra* note 609, at 124.
[630] Criminal Code, R.S.C, (1985) c. C-46, §487.0195.
[631] Sarit K Mizrahi, *supra* note 491, at 125.

from Online Crimes Act, 2014[632] was enacted hastily as a reaction to a tragic case of cyber bullying, and has caused to overlook privacy implications by significantly increasing the scope for law enforcement to request data from intermediaries.[633] Even though the higher level judiciary attempts to address the metaphor problem, the Canadian Parliament on the other hand is equivocal and ambiguous with regard to its purpose and intent.

ii. Finding an Investigative Necessity for Data in Motion

In case of interception, the law attempts to place procedural safeguards that are proportional to the intrusiveness of a Section 8 search.[634] To intercept, additional to the requirements of a general warrant, the law enforcement must convince the judge that there is an investigative necessity to conduct such an interception. The law enforcement agencies either have to prove that other methods have been exhausted or are unlikely to succeed, or that they are impractical given the urgency of the matter.[635] It has been clarified by the Canadian SC that the investigative necessity need not always be the last resort but there is burden on the police to present an affidavit with all facts and circumstances concisely to make sure there are "reasonable and probable grounds" to believe such interception is necessary and legal.[636] These additional requirements do not however, apply to investigations on terrorist activities or investigations into criminal

---

[632] Protecting Canadians from Online Crimes Act, 2014, S.C. 2014, C-31.
[633] Robert Diab, *The Road Not Taken: Missing Powers to Compel Decryption in Bill C-59, Ticking Bombs, and the Future of the Encryption Debate* 57 ALTA L. REV. 267 (2019).
[634] Lee, *supra* note 609, at 126.
[635] Criminal Code, R.S.C, (1985) c. C-46, §185.
[636] R v. Araujo, (2000) 2 SCR 992, at ¶ 59.

organisations.[637] This exception was a result of "moral panic" in the wake of gang wars and terrorist activities and was a conscious attempt by the legislature to placate the citizens and assure them of their safety.[638] However, the scope of criminal organisations and terrorist activities have been vastly expanded by the legislature which practically allows the police to circumvent the investigative necessity requirement irrespective of such target being "associated" with such offences or not.[639]

Unlike the USA where there are clear provisions applicable to different types of services, Canada does not have such distinction. It is still ambiguous as to what provisions would apply for procuring text messages or email communications. An OCS provider such as WhatsApp, essentially acts as an intermediary who periodically produces text messages to two consumers and such type of service is a continuing service. If an officer needs access to the messages between two consumers, a general search warrant or an assistance order, cannot be squarely applicable to such service simply because the service provider performs the dual role of storing and also providing messaging services at all times. In this context, the Canadian SC[640] categorised such search and seizure as interception and ruled that it requires an assistance order and not a general search warrant The Canadian SC was however split as to its reasons, with three of the justices relying on

---

[637] Criminal Code, R.S.C, (1985) c. C-46, §186.
[638] Jim Cruess, *Cost of Admission: One Rubber Stamp-Evaluating the Significance of Investigative Necessity in Wiretap Authorisations after R v. Araujo*, 32 DAL J OF L STUDIES 55, 65 (2013).
[639] *Id.* at 66.
[640] R v. TELUS Communications & Co., 2013 SCC 16.

the fact that data was procured "during transmission", while the other two justices relied on the nature of warrant sought which in this case was "prospective".[641]

iii. Encryption and Assistance Order

Although an Assistance Order can mandate a third party/any person to provide technical assistance to the law enforcement, it is unclear as to whether it could be used to mandate decryption.[642] There has also not been an instance before the court where it was required to mandate a third party to break an encryption to assist the court's investigation. The Assistance Order, however, could be issued by the judge to compel the owner of the personal device to decrypt the phone. The Canadian SC, after asserting that such compulsion is nothing short of compelled speech, held that encryption and the laws against self-incrimination could not be used to completely prevent the access of law enforcement to material evidence.[643] Subsequent to an emphasis on this caveat, the Canadian SC after assessing the facts of the case, came to a different conclusion in the end by holding that in balancing the competing interests of the State's access to evidence and the target's right to remain silent, the latter survived.[644] Unlike USA, the courts in Canada have emphasised on deciding upon the question of self-incrimination and privacy on a case to case basis.

---

[641] Susan*, supra* note 616, 512.
[642] Steven Penney & Dylan Gibbs, *Law Enforcement Access to Encrypted Data: Legislative Responses and the Charter,* 63 MCGILL L J 201, 211 (2017).
[643] R v. Shergill, (2019) ONJC 54, ¶ 46.
[644] *Id.* at ¶ 132.

C. UNITED KINGDOM

The UK does not have a written constitution but has incorporated the rights in the European Convention on Human Rights [*hereinafter* "**ECHR**"].[645] Article 8 of the ECHR[646] protects the right to privacy of the citizens.[647] The threshold, however, for a state to reasonably intrude into one's privacy is determined by the legality, necessity and proportionality of the intrusion.[648] In assessing proportionality, it looks at whether relevant and sufficient reasons are advanced by the state concerned for justifying an intrusion.[649]A supplementary requirement that the ECHR requires for the intrusion to be reasonable is that it must be "reasonably foreseeable", *i.e.*, the citizens must be made aware in uncertain terms the instances in which the State would intrude into one's privacy.[650]

The framework of UK is recapitulated in Investigatory Powers Act, 2016. This Act was preceded by the Regulation of Investigative Powers Act, 2000 which was subject to severe criticism because it lacked provisions mandating judicial pre-authorisation of digital searches.[651]

---

[645] Human Rights Act, 1998 (Eng.).
[646] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5, Art.8.
[647] Joyce W Luk, *Identifying Terrorists: Privacy Rights in the United States and the United Kingdom*, 25 HASTINGS INT'L & COMP L REV 223, 248 (2002).
[648] Handyside v. The United Kingdom, [1976] ECHR 5, ¶49.
[649] *Id.*
[650] Big Brother Watch v. U.K., [2018] ECHR 722.
[651] *Id.* at 254.

i. Warrant Requirement for Content Information

The law does not contemplate any consent requirement from the subject of the investigation. ECHR jurisprudence broadly classifies search and seizure as 'covert' or 'coercive' surveillance.[652] In terms of covert surveillance the type of data to be accessed is classified and the law clearly distinguish between "content of communications"[653] and "communications data",[654] which corresponds to content and non-content information respectively. However, the text does not in any manner suggest a threshold except for such search to be necessary and proportional. Much of the burden of developing the proportionality test was left to the judiciary, which anyway is subjected to the principles propounded by the ECHR on the vires of proportionality test several times.[655]

Any warrant irrespective of the type of data sought to be procured needs to be authorised by the Judicial Commissioner before the same is authorised by the Secretary of State.[656] Even though there is an urgency exemption, the warrant must be approved by the Judicial Commissioner within three days of its issue failing which it ceases to be operative.[657]

---

[652] *See generally,* Bernard Keenan, *State Access to encrypted data in the U.K: The "Transparent" Approach*, COMM. L W REV. (2019), https://eprints.bbk.ac.uk/id/eprint/29734/, (last visited September 29, 2020) ("**Bernard Keenan**").
[653] Investigatory Powers Act 2016, cl. 261(6).
[654] *Id.* cl. 261(5).
[655] *See* The Sunday Times v. United Kingdom, Eur. Ct. H. R. 49 (1979); Handyside v. The United Kingdom, Eur. Ct. H. R. 48 (1976).
[656] Investigatory Powers Act 2016, cl. 23.
[657] *Id.* at cl. 24.

ii. Encryption

Encryption engages the provisions regarding 'coercive' surveillance where the third party or the accused himself is coerced into decrypting the data obtained lawfully by the law enforcement.[658] The disclosure notice[659] in the Regulation of Investigative Powers Act mandates that the law enforcement could mandate either the third party or the target of the investigation to decrypt the data. The provision is applicable to a broad range of data defined as 'protected data' and to person who is in possession or control of the decryption key. The prosecution has the burden to prove that the key is in possession and control of the intended recipient of the notice; the recipient also has an opportunity to deny the same with adequate proof.[660]

Another mode of 'coercive' surveillance is by issuing the Technical Compatibility Notice [*hereinafter* "**TCN**"]. A TCN requires the service provider to grant technical assistance in any manner with the sole objective of ensuring that the intermediary has the ability to assist a lawful interception as long as it is reasonable and practicable to do so.[661] A TCN could be issued by the Secretary of the State only if it is authorised by a Judicial Commissioner.[662] The scope of TCN has been amplified under IPA

---

[658] Bernard Keenan, *supra* note 652, 20.
[659] Regulation of Investigatory Powers Act, 2000, § 49.
[660] STEPHEN MASON, ELECTRONIC SIGNATURES IN LAW (Cambridge University Press, 2012).
[661] Investigatory Powers Act 2016, cl.253.
[662] *Id.* at cl. 254.

and could be issued at any time irrespective of such notices complementing a disclosure notice or not.[663]

The England and Wales Court of Appeals held that compelling a person to produce the decryption key is similar to a key for a brief case or a purse, and the material inside the device would be intelligible and *"only be revealed for what it is"* as the key exists independent of the evidence (the contents of the briefcase/electronic device) itself.[664] The courts still emphasise on the need to prove that the person is in possession of the key.[665] The concept of self-incrimination is discussed in detail in the context of child pornography and terrorist acts, with the verdicts thus far being more or less in favour of the State.[666]

iii. Synthesising Lessons from other Jurisdictions

In comparing all these aforementioned foreign jurisdictions, we can clearly observe the different approaches these countries take in ensuring protection to privacy. Arguably these jurisdictions also fall short of an ideal framework. While USA and Canada have refrained from conclusively deciding on the question of encryption, the all-encompassing proportionality test in UK has subsumed and also theoretically justified, coercing subjects and third parties to provide passwords and decryption keys. However, USA's framework, even though fragmented, seems more

---

663 Bernard Keenan, *supra* note 652*,* 11.
664 R v. S, [2008] EWCA Crim 2177, ¶ 18.
665 *Id; see also* Greater Manchester Police v. Andrews, [2011] EWHC 1966 (Admin), ¶¶ 20-22.
666 Bela Chatterjee, *Fighting Child Pornography through UK Encryption Law: A Powerful Weapon in the Law's Armoury,* 24 CHILD & FAM L Q 410, 418 (2012).

sophisticated and tailored in addressing privacy concerns in digital searches, and above all there is correlation between the judge made law and legislations. On the contrary, Canada's framework presents a dichotomy of approach by the legislature and the judiciary, essentially cancelling out each other's effect rendering the law majorly ambiguous.

These differences could be attributable to the underlying differences in their search and seizure jurisprudence. It could also be attributable to the reluctance of topmost courts in Canada to specify tests and principles, which is also understandable given the dynamic nature of technology itself. As for digital searches, unlike India there are tailored procedures for each type of data or digital search/surveillance in all these countries. Lastly, none of these countries lack pre-judicial authorisation.

V. SUGGESTIONS: THE WAY FORWARD

A. ACKNOWLEDGING THE METAPHOR PROBLEM AND TAILORING PROCEDURAL SAFEGUARDS

As it could be inferred from the discussion above, the attempts by courts in USA, UK and Canada in addressing the metaphor problem could be attributable to the explicit provisions their constitutions regarding the negative obligation of the state in search and seizure. In the course of developing such privacy jurisprudence, a conscious attempt at understanding the implications on the right to privacy of a person in case of digital searches and distinguishing them from traditional searches seems to have been the first step in other jurisdictions.

The subsequent step would be to relinquish traditional rules and procedures followed in search and seizure and formulate new ones more appropriate for digital evidence. It is also argued that even specification of folders or locations within the cyber space in the warrant would be necessary to ensure that the digital search is "reasonable".[667] Minimization requirements within warrants were not considered a constitutional mandate, despite knowing that a digital search is more invasive because of the inherent contingency and unpredictability that a digital search and seizure entails.[668] However, the logic of the metaphor problem has managed to trickle down, and lower courts in the USA seem to be exercising the power to prescribe protocols and minimisation requirements as and when necessary.

Moreover, the impact of having recognized privacy as a fundamental right, on the search and seizure powers of the State has to be necessarily revisited. The procedure of search and seizure in India has not deviated much from the archaic pre-colonial principles and is significantly influenced by decisions of the Supreme Court immediately after independence.[669] Even in cases of interception, the courts and the law prevalent is significantly influenced and constrained by the guidelines formulated in *PUCL*. The very conflict between privacy and law

---

[667] Michael Mestitz, *Unpacking Digital Containers: Extending Riley's Reasoning to Digital Files and Subfolders,* 69 STAN L REV 321 (2017).
[668] Kerr, *supra* note 564, 575.
[669] *Kathi Kalu*, *supra* note 532; *M. P. Sharma*, *supra* note 516.

enforcement needs to be considered in light of the new *Privacy Judgement* and the techno-legal crisis that digital evidence presents.

B. ROLE OF THIRD-PARTY AND THE CONSENT REQUIREMENT

The case of *District Registrar & Collector v. Canara Bank*[670] has rejected the application of the third-party doctrine by expressly rejecting the *US v. Miller* case;[671] this was further affirmed by the *Privacy Judgement*.[672] However, in India the law enforcement has unconstrained access to data of citizens available with third parties. The provisions authorising such production are buried in the due diligence guidelines. This it is not only highly unsettling, but there arises a very important question as to whether such authorisation by the guidelines of the executive could be considered 'law' for the purpose of the proportionality test. In India, the legislature cannot delegate its essential functions, involving acts of laying down policy of the law and enacting that policy into a binding rule of conduct.[673] Considering the judgements by the Supreme Court on excessive delegations, it could be argued that entirely shifting the responsibility of protecting fundamental rights to the executive without any legislative guidance[674] is arbitrary and an excessive delegation of legislative powers and is thus, violative of Article 14 of the Constitution[675] as well.

---

[670] District Registrar & Collector v. Canara Bank, (2005) 1 SCC 496.
[671] Gautam Bhatia, *State Surveillance and the Right to Privacy in India: A Constitutional Biography,* 26 NAT'L L SCH INDIA REV 127, 151-152 (2014).
[672] *Privacy Judgement*, *supra* note 475, ¶ 77.
[673] In re The Delhi Laws Act, 1912, AIR 1951 SC 332; Hamdard Dwakhana v. Union of India, 1965 AIR SC 1167; M.L. Jain v. India AIR 1989 SC 669.
[674] Interception Rules, *supra* note 549, r. 4, 5, 8 & 22.
[675] INDIA CONST., Art.14.

The Supreme Court for the first time, albeit narrowly, had conceptualised privacy in terms of individual autonomy and liberty, and thereby striking down overbroad provisions in the U.P. Police Regulations that allowed for complete discretion to the police to enter any premises.[676] This moral argument for personal autonomy is crucial because later, in cases of balancing between right to free speech and right to privacy (private life), the Supreme Court[677] has held that even if a person's personal information is available to the public by way of their fame/position in society, materialisation of the same in any medium and the manner of the same could be justified only if the concerned person has given their consent. That is to say that the autonomous right to divulge one's personal information and the liberty to do so being guaranteed under Article 21, explicit consent plays an important role in justifying an encroachment, irrespective of such information being divulged voluntarily to any third party or the general public. Unfortunately, this consent requirement has not been inculcated in the search and seizure regime in India, due to the adherence to the Crime Control Model.

The Supreme Court in the case currently under consideration would hopefully decide on the broader question of the extent of assistance that the third party could be providing, procedural requirements and under what circumstances consent of the customer is necessary for a digital search to pass the test of proportionality as propounded in the *Privacy Judgement*.

---

[676] Gobind v. State of Uttar Pradesh, 1975 2 SCC 148, ¶ 24, 28.
[677] R. Rajagopal v. State of T.N., (1994) 6 SCC 632.

Given that consent by a subscriber of a particular service in respect of their personal information provided to the intermediary could never be equated to an informed consent,[678] using such consent to conclude that the citizen does not have reasonable expectation of privacy, as seen in Canada, is problematic. The courts in India must also take into consideration that such consent could not said to be given out of exercising their free will when it is "unwitting, coerced or incapacitated"[679] by extraneous pressures involved in making that decision. Which is why the consent requirement as stipulated in the USA could be a better choice in legitimising the procurement of digital evidence, *i.e.*, requiring consent before a seizure takes place, instead of transposing the consent given to intermediary as one that is indirectly given to the State.

C. ENCRYPTION- ANONYMITY UNDER ARTICLE 21

The judiciary would have to primarily decide on the extent of protection that Article 21 provides for anonymity. The 9-judge bench in the *Privacy Judgement* has clearly distinguished anonymity and privacy, but in terms of anonymized metadata and a legitimate state interest of procurement and perusal of the same (context of metadata and mass surveillance).[680] However, the ambit of Article 21 with respect to an

---

[678] Nupur Chowdhury, *Privacy and Citizenship in India: Exploring Constitutional Morality and Data Privacy*, 11 NUJS L REV 421, 426, 427 (2018); *see also, Justice Sri Krishna Committee Report, Free and Fair Digital Economy* (2019), 32-37, https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf (last visited September 9, 2020).

[679] Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent,* 96 WASH U L REV 1461, 1466 (2019).

[680] *Privacy Judgement*, *supra* note 475*,* ¶ 312.

individual and his expectation of anonymity in cyberspace has not been considered and delved into in the *Privacy Judgement* or thereafter. Canada has specifically entertained the notion that encryption shall not determine the existence of a reasonable expectation of privacy and that a requirement to decrypt would have to be determined on a case-to-case basis.[681] The judiciary in accommodating encryption and its privacy implications is also provided with the crucial task of choosing an appropriate metaphor.

In case of compelling the accused to produce the key, it depends on how the court interprets the act of providing the key by the accused.[682] The emphasis on what is being produced and equating it to a key for a safe box is problematic, as it disregards the role of the accused in rendering that information accessible and intelligible.[683] The courts in other jurisdictions discussed above have construed this conundrum in a manner where even when such compulsion would trigger the right against self-incrimination, it would still be construed as legitimate and reasonable compulsion.

The Supreme Court in *Kathi Kalu* has justified compulsion on the basis that such compulsion will not change the intrinsic character of the evidence. Applying the same logic, the content of the evidence already in existence and in possession of the police will not be altered in any manner by compelling the accused to produce the password. However, the role of the accused in incriminating himself and moreover in providing evidence

---

[681] Susan*, supra* note 616.
[682] *See generally,* Lex Gill, *supra* note 488.
[683] Bela Chatterjee, *Fighting Child Pornography through UK Encryption Law: A Powerful Weapon in the Law's Armoury,* 24 CHILD & FAM L Q 410, 419 (2012).

against himself under compulsion is completely disregarded, unlike the act-of-production doctrine followed in the USA. Moreover, the restriction of the scope of Article 22 to only testimonial evidence, could be revisited in light of the emergence of digital evidence.

D. JUDICIAL PRE-AUTHORISATION

The framework for judicial pre-authorization in USA is influenced by historical factors, refraining from adopting colonial laws and a heightened emphasis on citizen's privacy.[684] Granting such excessive powers to the executive is much less preferable when compared to the constitutional scrutiny of a neutral body like the judiciary.[685] Even in the UK the Investigatory Powers Act has adopted the system of prior judicial authorisation for the purpose of digital searches. However, in India, even though the law enforcement does have a 'legitimate state interest for the law to be reasonable; a neutral body by a mandatory *ex ante* warrant requirement overseeing digital searches is essential. Under no stretch of imagination could it be claimed that a procedure involving only the executive wing of the government to oversee and provide authorisations for law enforcement to infringe a citizen's fundamental right is a reasonable procedural safeguard.

---

[684] David G Barnum, *Judicial Oversight of Interception of Communications in the United Kingdom: An Historical and Comparative Analysis*, 44 GA J INT'L & COMP L 237, 292 (2016).
[685] *Id.* at 297.

E. LEGISLATIVE CLASSIFICATION OF TYPES OF DATA AND CLARITY IN LAW

The need for clarity in legislation which propounds to infringe upon one's privacy is mainly in adherence to the foreseeability principle, and the same has also been inculcated in India by the *Privacy Judgement*.[686] The Indian framework unlike the other jurisdictions does not acknowledge the different types of data that could help an investigation. Such classification is necessary for targeted procedural safeguards. It is desirable for such clarity to be present in the law, so that the citizens are aware of their rights and the procedures to be followed in a digital search. If the law framed is sufficiently precise to enable foreseeability, the judiciary would not be burdened in developing the law on case-by-case basis which is not only slower but could result in a lot of ambiguity and inconsistencies in the law.[687]

VI. CONCLUSION

The metaphor problem does not have a ready answer. It would even be a stretch to argue that the courts across the world have even understood the full extent and scope of the problem, or have successfully pre-empted the future problems that technological development could pose for digital searches and seizures. While the information that a person expects to keep private remains more or less the same throughout history, the vulnerability

---

[686] *Privacy Judgement*, *supra* note 475*,* 640.
[687] Timothy Azarchs, *Informational Privacy: Lessons from across the Atlantic,* 16 U PA J CONST L 805, 822 (2014).

and susceptibility of such information is robustly changing in the digital sphere. This paper has attempted to demonstrate the uncertainty and obscurity of the metaphor problem itself, which is captured by the subjective nature of the proportionality test used by UK, and the case-by-case approach adopted by the Canadian courts. While it is difficult to characterize the regime in USA, its attempt to objectively determine privacy right isn't entirely ideal.

This paper has also made efforts to explain in detail the great emphasis these legal systems place on procedural safeguards. It emanates from the fact that these legal systems have a constitutional mandate for reasonable search and seizure. On the contrary, in India due to the lack of any definitive notion of privacy, the law governing searches and seizures has evolved into a very oppressive regime, in juxtaposition to the other precocious legal systems discussed above. The author, analysing the legal system in India highlighted that the Supreme Court in the *Privacy Judgement*, does little to overcome *M. P. Sharma* and *Kathi Kalu,* which has assertively reinforced colonial notions of crime control post-independence. Problems such as lack of clarity in laws governing search and seizure, excessive delegation of powers to executive to adjudicate on matters of fundamental rights, inadequate if not absolute lack of procedural safeguards in respect of digital searches denotes excessive crime control. This is further aggravated by the fact that both the legislature and the judiciary in India is blind to the metaphor problem. Unless our legal system reforms radically to take account of these issues, it will render the right to privacy superficial.

NLUJ Law Review

Saumya Singh, *The Indian Judiciary, Domestic Violence and the Delusion of Rampant Misuse*, 8(1) NLUJ L. REV. 185 (2021).

THE INDIAN JUDICIARY, DOMESTIC VIOLENCE AND THE DELUSION OF RAMPANT MISUSE

ANALYSING THE JUDICIAL PERCEPTION REGARDING THE WIDESPREAD ABUSE OF DOMESTIC VIOLENCE PROVISIONS

*Saumya Singh**

ABSTRACT

The judicial perception regarding the widespread misuse of domestic violence provisions by women to harass and victimise innocent husbands and their relatives has been a mainstay in numerous judicial decisions. Over time, this perception has spurred a significant dilution of the procedural aspects of Section 498A of the Indian Penal Code, 1860 and a hesitance in registering cases under it. Further, it has spurred a summary disposal of complaints in some cases under Section 498A and the Protection of Women from Domestic Violence Act, 2005. This paper analyses this judicial perception. Through a critical analysis of the judgements echoing these concerns with respect to these laws, the paper examines the grounds on which this perception is based. The author argues that in inferring rampant misuse based on these grounds, the judiciary has acted in ignorance of the various social and legal barriers faced by

* The author is a third-year student at National Law School of India University and may be contacted at **saumyasingh@nls.ac.in**.

women in accessing and seeking justice from the legal system. The author further examines the reasons for the persistence of this perception in both public and judicial discourse, and traces this persistence to the patriarchal social structure that this perception both stems from and serves to maintain. The paper is concluded by highlighting the need for the judiciary to explicitly recognise the untenability of this perception, and to overrule the extant procedural dilutions.

TABLE OF CONTENTS

I. INTRODUCTION

The Indian society has traditionally had very strong patriarchal norms across communities, with women being accorded a very low social status.[688] In many communities, women have been viewed as the property of the father or the husband.[689] For example, Brahmanical texts such as the Manusmriti reflect such a conception.[690] Such patriarchal norms engender the ideas of control and subordination of women[691] and consequently, there has been a high prevalence of domestic violence against women in India.[692] Its pervasiveness is apparent from the findings of the National Family Health Survey 4, which has noted that 30% of women in India in the age group of 15-49 years have faced physical or sexual violence.[693] Domestic violence has further witnessed an alarming increase in the recent months, with the onset of the COVID-19 pandemic and the consequent imposition of a nationwide lockdown.[694]

---

688 Rehan Abeyratne and Dipika Jain, *Domestic Violence Legislation in India: The Pitfalls of a Human Rights Approach to Gender Equality*, 21(2) JOURNAL OF GENDER, SOCIAL POLITY & THE LAW 333, 336 (2012) ("**Abeyratne and Jain**").

689 *See id.*

690 *See* G BUHLER, THE LAWS OF MANU 195 (Oxford 1886).

691 Sonali Aggarwal, *Patriarchy and Women's Subordination*, 5(4) BHARTIYAM INTERNATIONAL JOURNAL OF EDUCATION AND RESEARCH 59, 59 (2016).

692 *See* Abeyratne and Jain, *supra* note 688, at 336- 337; Judith G Greenberg, *Criminalizing Dowry Deaths: The Indian Experience*, 11(2) JOURNAL OF GENDER, SOCIAL POLICY & THE LAW 801, 811 (2002).

693 INDIAN INSTITUTE FOR POPULATION SCIENCES, NATIONAL FAMILY HEALTH SURVEY 4 (NFHS-4) 2015-16 VOLUME 1 567 (IIPS 2017).

694 Kanika Arora and Shubham Kumar Jain, *Locked-down: Domestic Violence Reporting in India during COVID-19*, OXFAM INDIA (August 3, 2020), https://www.oxfamindia.org/blog/locked-down-domestic-violence-reporting-india-during-covid-19.

Recognising the scale and intensity of the problem, the Parliament of India has passed various laws to curb this menace and provide the survivors with remedies. Over time, Section 498A of the Indian Penal Code, 1860[695] [*hereinafter* "**IPC**"] and the Protection of Women from Domestic Violence Act, 2005[696] [*hereinafter* "**DV Act**"] have been enacted. These provisions have gradually broadened the scope of the legal protection available to women in terms of domestic relationships and abusive conduct covered, the remedies available, and the positive obligations on part of the State to take measures against domestic violence. However, the effectiveness of these laws has been stultified by, *inter alia*, various implementational issues. The judicial perceptions of domestic violence constitute one such issue. Such perceptions have influenced the interpretation and application of the various domestic violence provisions and have arguably militated against the efficacy of the same.

This paper analyses the tenability of one such judicial perception: that the various domestic violence provisions have been heavily misused by women, and have led to the victimisation of innocent husbands and their relatives. It focuses on both Section 498A and the DV Act, as this concern has been expressed very frequently in judgements involving both these provisions, and has significantly influenced adjudication where they are implicated, as has been discussed in this paper. While there has been some

---

695 The Indian Penal Code, 1860, No. 45, Acts of Parliament, 1860, § 498A (India) ("**the IPC**").

696 The Protection of Women from Domestic Violence Act, 2005, No. 43, Acts of Parliament, 2005, (India) ("**the DV Act**").

analysis on this perception and its tenability in the existing literature, there have been certain gaps in the same.

First, the extant analysis has focused squarely on analysing this judicial perception and its tenability with respect to Section 498A. However, the same has consistently found expression in cases concerning the DV Act as well, and has influenced adjudication through spurring unwarranted summary disposals of cases, as will subsequently be discussed. Further, the untrammelled prevalence of this perception with respect to the DV Act can potentially lead to calls for the dilution of its provisions from both within and outside the judiciary, as has been witnessed with respect to Section 498A. This is especially likely as the provisions of the DV Act have also been criticised as excessively broad in some judgements, as will be discussed. Hence, there is a need to examine the grounds advanced in support of the perception of rampant misuse in the relevant DV Act judgements, and whether the claim is reasonable.

Secondly, even with respect to Section 498A, the only ground relied on by judges for this perception that has been sufficiently analysed in the existing literature is that of high acquittal rates. However, there have also been other grounds that have formed the basis of this perception, which need to be critically examined to conclusively determine its tenability and whether it should influence adjudication.

Lastly, there has been insufficient analysis of the reasons for the rise and persistence of this perception in both public and judicial discourse

despite the absence of any concrete data supporting it, or of the patriarchal interests served by it.

This paper endeavours to build on the existing literature through conducting analysis on these aspects. It identifies and examines the three grounds relied on by judges for the perception and shows how these grounds do not support the same. In this regard, the paper analyses the various social and legal barriers that women face in both approaching and seeking justice through the legal system. It argues that these barriers preclude the possibility of any widespread misuse of the laws. In the light of its findings, the paper further analyses the reasons for the persistence of this perception in both public and judicial discourse despite its untenable nature. It traces this persistence to the patriarchal social structure that it stems from. Further, it also attributes such persistence to the critical role that the perception has played in maintaining this patriarchal structure, such as by enabling the systematic dismantling of the legal protection available to women. The paper concludes by highlighting the need for the judiciary to explicitly recognise the untenable nature of this perception, especially given the absence of concrete data affirming the same. Such a recognition is crucial especially in the light of the deleterious impacts of the reliance on this perception for the enforcement of domestic violence provisions.

II. THE JUDICIAL PERCEPTION REGARDING THE WIDESPREAD MISUSE OF DOMESTIC VIOLENCE PROVISIONS

Understanding the context and content of the two domestic violence laws is crucial for analysing the perception regarding their misuse.

Section 498A, the first provision in India dealing with domestic violence, was enacted in 1983.[697] It criminalised the treatment of a married woman by her husband and/or his relatives, with 'cruelty'.[698] 'Cruelty' includes harassment meted out to married women in connection with demands for dowry.[699] However, it also includes instances of domestic abuse that are unrelated to dowry, if the same are likely to drive the woman to commit suicide, or cause a "*grave injury or danger*" to the physical or mental health of the woman.[700] Procedurally, the offence defined by the provision is (a) cognisable and (b) non-bailable. This means that (a) arrest can be undertaken without the warrant of the magistrate, under Section 41 of the Criminal Procedure Code, 1973 [*hereinafter* "**CrPC**"], and (b) bail can only be granted by the courts.[701]

The scope of 'domestic violence' was expanded through the enactment of the DV Act. Recognising the multi-faceted nature of domestic violence, the DV Act broadened the scope of the conduct covered to include any conduct that causes physical, sexual, verbal, emotional, or economic abuse.[702] The standard of 'grave' danger or injury, as provided under Section 498A, has also not been included under the DV Act. Further, the DV Act is broader in terms of the domestic relationships

---

[697] Sawmya Ray, *Legal Constructions of Domestic Violence*, 55(3) SOCIOLOGICAL BULLETIN 427, 430 (2006).
[698] The IPC, § 498A.
[699] *See id.* explanation (b).
[700] *See id.* explanation (a).
[701] Abeyratne and Jain, *supra* note 688, at 354-355.
[702] The DV Act, § 3.

it covers, going beyond marriage to include relationships by consanguinity, adoption, etc.[703] Moreover, unlike Section 498A, which provides only criminal remedies, the DV Act provides for civil remedies such as protective orders and injunctions against the respondent(s).[704] It also envisions the implementation of protective measures on part of the State, such as the appointment of Protection Officers, to help women gain access to the legal system.[705]

Hence, there has been a gradual broadening of the scope of the provisions related to domestic violence in India, on various aspects. However, among some sections, this increase in scope has stoked a concern regarding the misuse of the provisions by women, to harass innocent husbands and their relatives.[706] Even in the absence of concrete data backing such claims,[707] these concerns have increasingly dominated the public sphere, and have even been expressed by judges at various levels.

Section 498A is one provision for which judges have expressed such concerns. In some cases, such as *Lalita Kumari v. Government of UP*,[708] which dealt with general guidelines regarding arrest in case of cognisable offences, the provision has been cited as exemplifying the registration of a

---

[703] *See id.* §2(f).
[704] Abeyratne and Jain, *supra* note 688, at 343; *see also* the DV Act, §§ 18-23.
[705] Abeyratne and Jain, *supra* note 688, at 343; The DV Act, §§ 8, 10, 11.
[706] Biswajit Ghosh and Tanima Choudhuri, *Legal Protection against Domestic Violence in India: Scope and Limitations*, 26 JOURNAL OF FAMILY VIOLENCE 319, 322-323 (2011) ("**Ghosh and Choudhuri**").
[707] *See* note 735.
[708] Lalita Kumari v. Government of UP and Ors, (2014) 2 SCC 1, ¶ 27, 28 ("***Lalita Kumari***").

large number of frivolous complaints. Other judgements have dealt squarely with Section 498A and expressed concern regarding the rampant misuse of the same. The provision has been called a "*weapon… by disgruntled wives*",[709] used in a "*cruel, ruthless, and totally revengeful manner*"[710] and possibly causing "*legal terrorism*" [711] and "*hitting at the foundations of marriage*".[712] The women allegedly misusing the provision have been termed as "*wolves masquerading in the human flesh*" who must be "*dealt with iron hand*".[713]

The judicial perception of rampant misuse has also found expression in cases relating to the DV Act, such as *Loha v. The District Educational Officer*.[714] Different courts have raised concerns about the Act being invoked by wives to "*terrorise the husbands, their families and distant relatives*"[715] in order to "*vent their personal vendetta and stake a claim in the properties belonging to the husband and the in-laws*".[716]

In the context of Section 498A, the Supreme Court of India [*hereinafter* "**the Supreme Court**"] has held the threat of misuse to be insufficient to affect the constitutionality of the provision.[717] However, the perception of rampant abuse has influenced decisions regarding the

---

[709] Arnesh Kumar v. State of Bihar, (2014) 8 SCC 273, ¶ 6 ("***Arnesh Kumar***").
[710] Social Action Forum for Manav Adhikar v. Union of India, Ministry of Law and Justice and Others, (2018) 10 SCC 443, ¶ 1 ("***Social Action Forum***").
[711] Sushil Kumar Sharma v. Union of India, (2005) 6 SCC 281, ¶ 18 ("***Sushil Kumar***").
[712] Savitri Devi v. Ramesh Chand and Others, 2006 (3) WLC 332, ¶ 21 ("***Savitri Devi***").
[713] *Id.* ¶ 28.
[714] Loha v. The District Education Officer, WP (MD) No 8646 of 2015, ¶¶ 5-6 ("***Loha***").
[715] Anoop and others v. Vani Shree, 2014 SCC OnLine P&H 14730 ("***Anoop***").
[716] Bhartiben Bipinbhai Tamboli v. State of Gujarat, 2018 SCC OnLine Guj 9, ¶ 23 ("***Bhartiben***").
[717] *Sushil Kumar*, *supra* note 711, ¶ 13.

procedure to be followed while implementing the same, especially during arrest. Hence, in *Arnesh Kumar v. State of Bihar*,[718] the Supreme Court laid down guidelines regarding arrests in the case of cognisable offences involving a potential imprisonment of less than, or equal to, seven years. Even though the guidelines were also applicable to other offences,[719] they were framed with an eye on Section 498A, with only the misuse of this provision being analysed in the judgement. The concern regarding widespread misuse also led the Court to consider "*matrimonial disputes/ family disputes*" as fit for a 'preliminary inquiry' into complaints by the police.[720] Such inquiries are focused on ascertaining whether the information provided in the First Information Report reveals the commission of a cognisable offence.[721] Hence, the Supreme Court has effectively created a mechanism for the police to screen Section 498A complaints, based on their opinions of whether an offence under the provision has been committed.

The saga of procedural dilutions culminated with the Supreme Court's judgement in *Rajesh Sharma v. State of UP* [*hereinafter* "***Rajesh Sharma***"],[722] with the Court laying down expansive guidelines specifically for the investigation and prosecution of Section 498A complaints not involving physical injuries and death.[723] The same included various unique

---

[718] *Arnesh Kumar*, *supra* note 709
[719] *Id.* ¶ 14.
[720] *Lalita Kumari*, *supra* note 708, ¶¶ 27-28, 111.
[721] *Id.* ¶ 111.
[722] Rajesh Sharma v. State of UP, 2017 SCC Online SC 82 ("***Rajesh Sharma***").
[723] *Id.* ¶ 19.

measures, such as the constitution of a 'Family Welfare Committee' to examine the validity of every complaint before the commencement of the usual criminal procedure.[724] The severe dilution in procedural requirements undertaken in this judgement was heavily criticised by scholars.[725] Further, some of these measures, including the one mentioned, were such significant departures from the CrPC that they were overruled by the Supreme Court later. The ground for the overruling, however, was the inconsistency of the same with the CrPC,[726] and not that *Rajesh Sharma* had overestimated the extent of misuse and acted disproportionately. In fact, some of the guidelines laid down in *Rajesh Sharma* were upheld for being "*protective in nature*",[727] and continue to remain part of the criminal procedure for Section 498A cases. These include the general exemption for the family members of the accused husband from physical appearance in trial courts, and the rule that Red Corner Notices should generally not be issued to Non-Resident Indians in Section 498A cases.[728] The trial courts had earlier

---

[724] *See id.*

[725] Bindu N. Doddahatti, *The Dangerous, False Myth That Women Routinely Misuse Domestic Cruelty Laws*, THE WIRE (August 11, 2017), https://thewire.in/gender/section-498a-domestic-cruelty-laws (provides one such critique of the judgement in *Rajesh Sharma*). ("**Doddahatti**")

[726] Social Action Forum, *supra* note 710; *see* also Rajesh Sharma, *supra* note 722, ¶ 19(i) and CODE CRIM. PROC. § 154; *Rajesh Sharma*, *supra* note 722, ¶ 19(iii) and CODE CRIM. PROC. § 482.

[727] Social Action Forum, *supra* note 710, ¶ 35.

[728] *Rajesh Sharma*, *supra* note 722, ¶ 19. Red Corner Notices are notices published by the Interpol on the request of countries' National Central Bureaus, requesting for the arrest of an offender with a view to subsequent extradition: *Interpol*, CENTRAL BUREAU OF INVESTIGATION, https://cbi.gov.in/Interpol-Notices#a.

enjoyed discretion with respect to these decisions, based on the facts of the case.[729]

The perception of the widespread misuse has hence had a considerable bearing on the judicial dilution of the procedure to be followed in the implementation of Section 498A. Further, such a deep-rooted concern has potentially influenced the adjudication on merits of both Section 498A and DV Act cases, and made judges more suspicious in accepting the prosecution's/petitioner's case. Such a tendency is patent in *Loha v. The District Educational Officer*,[730] where a "*bare reading*" of the petitioner's affidavit was considered sufficient to infer the misuse of the DV Act by her against her father-in-law, without examining any other relevant evidence regarding the complaint.[731] In the case of the police, the repeated assertion of this concern in judicial pronouncements has led to their rationalising their inaction in carrying out Section 498A arrests through quoting the said judicial decisions.[732] Even the government has bought into this narrative and has directed the police to register Section 498A complaints only as a last resort, after first attempting reconciliation through various counselling and mediation measures.[733] To justify this direction, it has cited "*some cases*" of the misuse of the provision.[734] Hence,

---

729 *Social Action Forum*, *supra* note 710, ¶¶ 21-22.
730 *Loha*, *supra* note 714.
731 *Id.* ¶ 7.
732 *See Social Action Forum*, *supra* note 710, ¶ 10.
733 *Victimised Twice Over*, 44(46) EPW 6, 7 (2009); *Misuse of Section 498A- regarding*, MINISTRY OF HOME AFFAIRS (October 20, 2009), https://www.mha.gov.in/sites/default/files/Adv498_220114_0.PDF.
734 *See id.*

there is a need for assessing the basis and tenability of this judicial perception.

III. AN ANALYSIS OF THE GROUNDS FORMING THE BASIS OF THIS JUDICIAL PERCEPTION

The judicial perception regarding the widespread misuse of Section 498A and the DV Act is not based on any concrete data regarding the extent of the misuse of the provisions, for these exists insufficient data on this point to reach conclusions regarding rampant abuse.[735] In fact, in the context of Section 498A, the existing limited data has pointed to the absence of the rampant misuse of the provision. For example, an analysis of the National Crime Records Bureau data from 2005 to 2009 has revealed that only 9-10% of the cases filed under Section 498A in the period were false in terms of being driven by a mistake of law or fact.[736] An empirical study conducted by the Centre for Social Research has also pointed to a minimal percentage of the examined complaints being found false during investigation (specifically, 6.5%).[737] The lack of sufficient empirical data has even led to a petition by 'men's rights activists' to the Government, to

[735] In the context of Section 498A, *see* Abeyratne and Jain, *supra* note 688, at 358-359 and LAW COMMISSION OF INDIA, REPORT NO. 243: SECTION 498A IPC (2012) 3. As recently as 2018, the absence of sufficient concrete data was also highlighted by the petitioner in *Social Action Forum*, *supra* note 710, ¶ 8, and the argument was not rebutted by the respondents or the Court.

[736] Swayam, Kolkata, *Section 498A: A Report Based Upon Analysing Data From the National Crime Records, 2005-2009,* PLD INDIA (August, 2011), https://feministlawarchives.pldindia.org/wp-content/uploads/498A-Report-for-NCW-final.pdf.

[737] Abeyratne and Jain, *supra* note 688, at 358.

collect the same.[738] In the absence of data affirming the judicial perception of rampant abuse, the judicial decisions expressing concerns over the same primarily base their perception on three grounds:

(A) The alleged over-breath of the provisions, and the consequent ability of the same to be misused;
(B) The existence of individual cases of misuse;
(C) The high acquittal rate in Section 498A cases.

While the first two grounds have been adopted in cases relating to both Section 498A and the DV Act, the third ground has been prevalent in judgements relating to Section 498A. It hence becomes necessary to analyse if any of these grounds lends credence to the concerns of the judges. The first two grounds will be analysed together, in the first sub-section. The third ground will be examined in the second sub-section. This separation in analysis has been undertaken as the discussion of these grounds requires an examination of different sets of factors. As will subsequently be discussed, a critical analysis of grounds *(A)* and *(B)* necessitates an examination of the structural barriers faced by women in approaching the legal system and filing Section 498A or DV Act complaints in the first place. While these barriers have been discussed in existing literature, the analysis of these two grounds and whether they necessitate an inference of rampant misuse has not yet been undertaken. On the other hand, the examination of ground

---

[738] *To obtain reliable data by conducting empirical study on misuse of provisions of 498-A IPC*, CHANGE.ORG., https://www.change.org/p/ministry-of-home-to-obtain-reliable-data-by-conducting-empirical-study-on-misuse-of-provisions-of-498-a-ipc?recruiter=681006065&recruited_by_id=ac203790-f0dd-11e6-9c51-99246b9ffc02.

(C) merits a consideration of the barriers faced in obtaining Section 498A convictions even in genuine cases once complaints have been filed.

A. THE ALLEGED OVER-BREATH OF THE PROVISIONS CONCERNED, AND THE EXISTENCE OF INDIVIDUAL CASES OF MISUSE

In some cases, the allegedly wide scope of the provisions is cited as a factor that, as per courts, makes them prone to misuse. Hence, in the context of the DV Act, the Madras High Court held that the ability of the provisions to be misused would make women use the same to "*teach a lesson*" to husbands and their relatives.[739] In the context of Section 498A, the Supreme Court has expressed concerns of over-breath through arguing that the provision effectively vests police officers with the determination of the contours of 'cruelty' and 'harassment',[740] and even courts have struggled to reach "*safer conclusion*" regarding the same.[741] This perception of over-breath, as well as the existence of individual cases of (alleged) misuse, have also potentially influenced the judicial approach in the cases where broad generalisations regarding rampant misuse are made without citing any concrete data. Such generalisations have been observed in judgements pertaining to both Section 498A[742] and the DV Act.[743] Even the Malimath

---

[739] *Loha*, *supra* note 714, ¶ 6.
[740] *Savitri Devi*, *supra* note 712, ¶¶ 21, 25.
[741] *Id.* ¶ 21.
[742] *Sushil Kumar*, *supra* note 711 and Preeti Gupta and Another v. State of Jharkhand and another, (2010) 7 SCC 667 ("***Preeti Gupta***").
[743] *Anoop*, *supra* note 715 and Bhartiben, *supra* note 716, at ¶ 23.

Committee expressed apprehensions about the widespread misuse of Section 498A without citing any statistics.[744]

Scholars have agreed that the provisions related to verbal abuse in the DV Act could have been defined more specifically, with a further definition or standard clarifying the contours of 'insults' and 'ridicule'.[745] However, the breath of the other provisions defining domestic violence cannot be assailed. Broad provisions defining domestic violence are necessary given its the multi-faceted nature, and the need for broad definitions to cover various types and instances of abusive conduct.[746] In any case, merely the breath of the domestic violence provisions and the existence of individual cases of misuse cannot be valid grounds for reaching definite conclusions regarding the rampant misuse of the provisions. In concluding so, the courts have acted in ignorance of the various social factors that deter even genuine domestic violence complaints in India. Available data show that only under 1% of married women facing domestic violence have been able to file criminal complaints,[747] and only in the most extreme of cases.[748] In such a social scenario, the rampant abuse of Section

---

[744] DR. JUSTICE V.S. MALIMATH COMMITTEE ON REFORMS OF CRIMINAL JUSTICE SYSTEM, MINISTRY OF HOME AFFAIRS, REPORT VOLUME I (March, 2003) ¶ 16.4.4.
[745] Ghosh and Choudhuri, *supra* note 706, at 323.
[746] Sanjay Ghose, *Supreme Court Order on Domestic Abuse Cases Is a Step Back for Women's Rights Law*, THE WIRE (July 31, 2017), https://thewire.in/gender/supreme-court-domestic-abuse-dowry ("**Ghose**").
[747] Doddahatti, *supra* note 725.
[748] Shalini Nair, *498A, battered*, THE INDIAN EXPRESS (June 26, 2018), https://indianexpress.com/article/india/498a-battered-supreme-court-misuse-of-dowry-law-women-harassment-cruelty-sneha-sharma-allahabad-hc-4794220/.

498A or the DV Act on the scale exhorted by the courts is highly improbable at best.

There is a general lack of government efforts to raise awareness of the laws, and implement the protective measures prescribed under the DV Act.[749] This contributes to the lack of awareness of the provisions among women.[750] The lack of awareness generation has particularly posed a significant barrier in accessing the legal system for women from underprivileged backgrounds. This was noted in a study conducted in Burdwan in West Bengal, where most cases filed under the DV Act were filed by women from urban backgrounds who had access to the services of lawyers.[751] However, even women who are aware of the relevant legal provisions face various barriers in seeking justice, making even the use of the provisions in genuine cases extremely difficult, much less misuse.

Firstly, traditional patriarchal norms privilege the maintenance of family and marriage over the rights of the woman. Under the influence of such norms, various actors in the legal system, from the police[752] to the Protection Officers appointed under the DV Act,[753] have placed heavy

---

[749] Ghosh and Choudhuri, *supra* note 706, at 324.
[750] *See id.*
[751] *See id.*
[752] Sowmya Rajaram and Jayanthi Madhukar, *One step forward, two back*, BANGALORE MIRROR (August 27, 2017), https://bangaloremirror.indiatimes.com/opinion/sunday-read/one-step-forward-two-back/articleshow/60239078.cms; Prashant K Trivedi and Smriti Singh, *Fallacies of a Supreme Court Judgement: Section 498A and the Dynamics of Acquittals*, 49(52) ECONOMIC AND POLITICAL WEEKLY 90, 94-95 (2014) ("**Rajaram and Madhukar**").
[753] Aarefa Johari, *Twelve years since the Domestic Violence Act, how well do protection officers help women in need?*, SCROLL (March 28, 2017), https://scroll.in/article/830882/twelve-years-

emphasis on the re-conciliation of the couple. In some cases, women seeking legal recourses against domestic violence have been exhorted to return to the abusive household to prevent the fragmentation of the family.[754] This overriding concern with preserving the family has found expression even in various judicial decisions, including those of the Supreme Court. One of the grounds on which the courts have criticised the alleged rampant misuse of domestic violence provisions is that *"thousands of marriages have been sacrificed at the altar of this provision*",[755] and that it stifles any potential reunion of the couple.[756] The prioritisation of the family over the women's dignity and rights is also reflected in the nomenclature of the Family Welfare Committees sought to be set up in *Rajesh Sharma*.[757] For women, the internalisation of this emphasis on the preservation of the family has often led to their accepting domestic violence without seeking legal recourses, to keep the marriage together.[758] In such a social situation, the widespread abuse of the laws is highly unlikely.

Secondly, the performance of state governments in appointing Protection Officers under the DV Act has been dismal at best. Most states

---

since-the-domestic-violence-act-how-well-do-protection-officers-help-women-in-need. ("**Johari**")

754 Ghose, *supra* note 746.

755 *Savitri Devi*, *supra* note 712, ¶ 23.

756 *Rajesh Sharma*, *supra* note 722, ¶ 7.

757 Deva Bhattacharya, *Domestic Violence: Supreme Court verdict on Section 498A puts family honour over women's rights*, FIRSTPOST (July 29, 2017), https://www.firstpost.com/india/domestic-violence-supreme-court-verdict-on-section-498a-puts-family-honour-over-womens-rights-3870627.html.

758 *Shades of Courage: Women & Indian Penal Code Section 498A*, TATA INSTITUTE OF SOCIAL STUDIES (1999), https://www.tiss.edu/uploads/files/6Shades_of_Courage.pdf.

have appointed fewer than the required officers, and some appointments have been carried out merely through assigning additional duties to the existing officers.[759] Even where Protection Officers have been appointed, there have sometimes been issues with their approachability and functioning, such as the lackadaisical attitude of the officer concerned towards the complainant's case.[760] This has deprived women of a significant outreach mechanism envisioned under the DV Act to enable them to access the legal system.

Thirdly, in many families, domestic violence is perceived as normal, with inferiority and submission on the part of women being promoted by the patriarchal social structure.[761] Further, violence is often advocated as a disciplinary measure against wives by in-laws, often by the mother-in-law herself.[762] The internalisation of such norms deters women from approaching the authorities in even extreme domestic violence cases, much less for filing vexatious complaints.

Fourthly, cultural practices such as patrilocal residence and the sexual division of labour often make women heavily dependent on their husband's families for subsistence.[763] In such situations, there is a strong disincentive to file cases against the husband, since the same might endanger the survival

---

[759] Ghose, *supra* note 746.
[760] Johari, *supra* note 753.
[761] Sujata Gadkar-Wilcox*, Intersectionality and the under-Enforcement of Domestic Violence Laws in India*, 15 UNIVERSITY OF PENNSYLVANIA JOURNAL OF LAW AND SOCIAL CHANGE 455, 470 (2012) ("**Gadkar-Wilcox**"); Trivedi and Singh, *supra* note 752, at 91.
[762] Gadkar-Wilcox, id. at 470-471.
[763] *Id.* at 465-466.

of the woman.[764] Patrilocal residence can exacerbate the problem by leading to the separation of women from their friends and family, who could have lent them economic and emotional support in the legal battle against the husband and his family.[765]

In such a social context, where there is such heavy deterrence for women to file even genuine complaints, the claim of disproportionately high false complaints becomes extremely difficult to sustain.

The inability to use domestic violence provisions and seek legal redress is heightened in the case of women belonging to lower castes or classes.[766] Even if women from these backgrounds are able to approach the authorities, they might not have the economic means to convince the authorities to prosecute cases, given the prevalence of bribery and corruption.[767] Further, these women are often discriminated against by the authorities because of their caste or class identity, and officers are hesitant and unwilling to file complaints brought by them.[768] Such a callous attitude of the authorities can prove to be a significant deterrent in filing complaints.[769] The lack of economic privilege also precludes women from these backgrounds from filing appeals.[770]

---

764 *See id.*
765 *Id.* at 471.
766 *Id.* at 466-469, 470-473.
767 *Id.* at 468.
768 *Id.* at 468, 470.
769 *See id.*
770 *Id.* at 468.

Hence, the social milieu of the country disadvantages women and militates against their seeking legal redress, in even extreme domestic violence cases. Where the legal system is so unapproachable for even genuine complainants, the abuse of the legal process by women on the scale averred by the courts is highly unlikely. In such a situation, given the absence of concrete data affirming rampant misuse, the breath of the provisions or the existence of individual cases of misuse cannot form the basis of conclusions regarding rampant abuse.

B. THE HIGH ACQUITTAL RATES IN SECTION 498A CASES

In the context of Section 498A, the high acquittal rates in cases involving the provision have been cited in judgements as proof of its rampant misuse. For example, in *Arnesh Kumar v. State of Bihar*,[771] the Supreme Court justified its perception of misuse by citing National Crime Records Bureau data showing that the conviction rate in domestic violence cases in 2012 was only 15%.[772]

In interpreting this data to imply high levels of misuse of the provision, courts have assumed that acquittal is primarily the result of the frivolousness of the complaints. This assumption, however, becomes untenable when other factors causing such high rates of acquittal are analysed. There exist various lacunae in the implementation of Section 498A on part of various stakeholders in the criminal justice system, that

[771] *Arnesh Kumar*, *supra* note 709.
[772] *Id.* ¶ 6.

cumulatively result in multiple barriers for survivors of domestic violence to access justice and secure convictions under the provision.

In general, the lack of the implementation of training measures for police officials and judges regarding domestic violence has hampered the implementation of the provisions and convictions thereunder.[773] In the absence of such training, traditional conceptions of domestic violence, marriage and gender roles have dominated decision-making on part of both the police and the courts. On part of the police, domestic violence has often been attributed to the difficulties of adjusting to a new marriage, instead of viewing the same as reflective of a patriarchal social structure and male domination.[774] Often, the female survivor is blamed for the violent behaviour of the husband.[775]

Further, domestic violence has also been viewed as a 'private matter', best resolved within the family.[776] In some cases, even egregious instances of domestic violence are considered mere everyday 'incidents', and complaints are not registered.[777] Corruption also poses a significant barrier against access to justice. The police are often unwilling to pursue

---

[773] The DV Act, § 11(b); Abeyratne and Jain, *supra* note 688, at 351. Such training has been mandated not only with respect to domestic violence but also other offences that require social awareness and sensitivity for proper investigation and adjudication, such as rape. *See* PARTNERS FOR LAW IN DEVELOPMENT, TOWARDS VICTIM FRIENDLY RESPONSES AND PROCEDURES FOR PROSECUTING RAPE 50 (PLD 2015).
[774] Greenberg, *supra* note 692, at 811-13.
[775] *Id.* at 812-13.
[776] *See id.*
[777] *Id.* at 813.

domestic violence cases, especially those against influential persons.[778] Resultantly, owing to these factors, the investigation in domestic violence cases is often lackadaisical, and leads to judges dismissing cases for lack of evidence.[779] Hence, on the level of the police, there are significant barriers to the prosecution of domestic violence cases, contributing to the high acquittal rates.

Some of these conceptions also influence the courts in decision-making, hence adding to the barriers in securing convictions in Section 498A cases and fuelling the high acquittal rates. Subordinate courts are often unwilling to convict those accused of domestic violence, as is visible in their appreciation of evidence.[780] For example, a trial court acquitted the accused based on some discrepancies in the dying declaration of the deceased, even though eight prosecution witnesses testified to domestic abuse.[781]

The Supreme Court has noted the lackadaisical approach of the lower courts in enforcing domestic violence laws, with the accused being acquitted for untenable reasons.[782] Further, the conception of domestic violence as a transitory problem at the beginning of marriages is prevalent in the judiciary, including the Supreme Court. The continuation of marriage

---

[778] Abeyratne and Jain, *supra* note 688, at 351.
[779] Gadkar-Wilcox, *supra* note 761, at 464; *see id*., 351-352; *see also* V Elizabeth, *Patterns and Trends of Domestic Violence in India: An Examination of Court Records, in* INTERNATIONAL CENTRE FOR RESEARCH ON WOMEN, DOMESTIC VIOLENCE IN INDIA: A SUMMARY REPORT OF FOUR RECORDS STUDIES 36, 38 (2000).
[780] Gadkar-Wilcox, *supra* note 761, at 464.
[781] *See id.*
[782] Narsingh Prasad Singh v. Raj Kumar, (2001) 4 SCC 522 ("***Narsingh***").

in such cases is often the judicially favoured outcome. This perception was reflected in *Preeti Gupta v. State of Jharkhand*,[783] where the Supreme Court exhorted lawyers not to take up 'frivolous' cases so as to maintain the "*social fibre, peace and tranquillity of the society*".[784] Another perception relating to domestic violence that is prevalent among judges and proves a significant barrier in obtaining Section 498A convictions, is that of domestic violence being a 'private matter' best settled within the family. Even the Supreme Court has treated domestic violence as an offence of "*overwhelmingly and predominatingly civil flavour*", best settled through 'reconciliation'.[785] Since such 'settlements' are implemented by the high courts through quashing the complaints under Section 435 of the CrPC, they increase the number of acquittals under Section 498A, even where the original complaint is genuine.[786] Moreover, even though Section 498A recognises physical and mental cruelty as a separate form of cruelty unconnected with dowry harassment, judges still look for evidence of the latter, and dismiss cases in the absence of the same.[787] Judges sometimes also base their decision on the cause of the violence rather than focussing on the violent act itself.[788] Hence, untenable judicial perceptions relating to domestic violence are a significant reason for the high acquittal rates under Section 498A; these data

---

[783] *Preeti Gupta*, *supra* note 742.
[784] *Id.* ¶ 31.
[785] Gian Singh v. State of Punjab, (2012) 10 SCC 303, ¶ 61.
[786] Rajaram and Madhukar, *supra* note 752.
[787] Ray, *supra* note 697, at 433-434; *see also* Richhpal Kaur v. The State of Haryana and Anr., (1991) 2 RCR (Cri) 53.
[788] *See id.*

can therefore not be summarily chalked off as a product of widespread misuse.

In addition to the perceptions relating to domestic violence that pervade the legal system, the difficulty of sourcing evidence regarding the offence also stymies the enforcement of Section 498A. Often violence occurs within the house, and obtaining proof of the same is very difficult, for members of the household are socialised to refrain from testifying about 'private matters' to maintain the honour and dignity of the family.[789] Sourcing medical evidence has also become difficult where doctors have refused to submit reports of the woman's injuries, to prevent themselves from becoming involved in the legal proceedings.[790] Moreover, even where evidence is available, judges are often unwilling to enforce domestic violence provisions. In many cases, this leads to untenable approaches in the examination of the evidence.[791] Sometimes, judges dismiss dying declarations on the grounds on the unfit mental condition of the woman, even when the same has been verified by medical experts.[792] Witnesses are declared as hostile in the presence of slight variations in their statements.[793] Overall, the problem of evidence is acute enough to make proving the relevant facts extremely difficult.

---

[789] Ray, *supra* note 697, at 435.
[790] Rajaram and Madhukar, *supra* note 752.
[791] Gadkar-Wilcox, *supra* note 761, at 464; Narsingh, *supra* note 95.
[792] Ray, *supra* note 697, at 436; *see also* Ramesh and Others v. State of Haryana, (2017) 1 SCC 529, ¶¶ 1-3, 18, 18.1, 20, 21, 30, 34-35.
[793] Ray, *supra* note 697, at 438.

Hence, on the level of implementation, there are various issues that plague Section 498A. Implementation has significantly been hindered by the traditional and patriarchal conceptions of domestic violence, marriage, and gender roles among the police and judges. Further, many cases of acquittal have resulted from the abandonment or withdrawal of the prosecution by wives, owing to various factors including familial and police pressure[794] and financial constraints.[795] The high acquittal rates in domestic violence cases can hence not be interpreted to signal high levels of misuse of Section 498A. It is therefore erroneous to rely on these data to reach conclusions regarding widespread abuse of the provision, as has been done by the courts.

IV. THE ROOTS OF THIS PERCEPTION OF RAMPANT MISUSE, AND THE PATRIARCHAL INTERESTS SERVED BY IT

The perception of the rampant misuse of Section 498A and the DV Act is hence untenable in the light of concrete data and the lived experiences of women with the legal system. Nevertheless, it has consistently formed a mainstay of both public and judicial discourse regarding domestic violence. Perhaps unsurprisingly so, for this perception finds its roots in the patriarchal structure of the Indian society, and the

[794] Ghose, *supra* note 746; Jayna Kothari, *Criminal law on Domestic Violence: Promise and Limits*, 40(46) ECONOMIC AND POLITICAL WEEKLY 4843, 4846 (2005).
[795] Trivedi and Singh, *supra* note 752, at 95.

misogynistic attitudes promoted by it towards women who approach the legal system. Further, the perception serves various patriarchal ends.

A significant facet of the Indian society across communities has been the pervasiveness of values and norms furthering the control and subordination of women.[796] Further, 'saving' families and marriages has consistently been privileged over the dignity and rights of women.[797] In such a social structure, submissiveness to marital and familial oppression is taken as the norm, and women who attempt to break the shackles and reach out to the legal system are perceived as deviants 'misusing' the law.[798] In various ways, their complaints are sought to be chalked off as instances of the abuse of the legal system, by actors both outside and within it. These include imputing various nefarious motives to complainants, branding them as 'oversensitive', and downplaying the violence faced by them as transient 'adjustment' problems.[799] Through 'settlements' and more recently, Family Welfare Committees, every attempt is made to save oppressive marriages and families, at the cost of women's rights and lives.

Besides stemming from the patriarchal social structure, this perception of rampant misuse significantly contributes to its maintenance. In two crucial ways, this perception has played a key role in turning the clock back with respect to the legal protection available to women, hence ensuring that patriarchal familial oppression is sustained.

---

[796] Aggarwal, *supra* note 691, at 59.
[797] Bhattacharya, *supra* note 757.
[798] Flavia Agnes, *Section 498A, Marital Rape and Adverse Propaganda*, 50(23) ECONOMIC AND POLITICAL WEEKLY 12, 13 (2015).
[799] Ghose, *supra* note 746.

Firstly, it provides a ground for legitimising heavy procedural dilutions, hence eating away at the efficacy of the legal provisions in ensuring justice in domestic violence cases. For example, in *Social Action Forum for Manav Adhikar v. Union of India* [*hereinafter* "***Social Action Forum***"], the Supreme Court did not find anything problematic in the substance of the guidelines laid down in *Rajesh Sharma*. On the contrary, they were perceived as preventing "*unfairness and unreasonableness*" by establishing a "*fair procedure*" for arrests and investigations in Section 498A complaints.[800] Hence, if the same are introduced again as a legislative measure, they will probably stand judicial scrutiny, effectively placing the woman's complaint hostage to the opinions of an untrained bunch of volunteers. Even at present, though the Family Welfare Committee mechanism stands dismantled, the work of screening complaints is instead effectively being undertaken by the police, through the 'preliminary inquiries' allowed by the Supreme Court to curb the alleged misuse. Another example of such significant procedural dilutions is the attempt by the various actors in the legal system, from the Law Commission of India[801] to the Union Government,[802] to make Section 498A compoundable and legally enable reconciliations in false or 'trivial' complaints. In the process, there has been a blatant disregard for the various forms of pressures faced

[800] *Social Action Forum*, *supra* note 710, ¶ 36.
[801] Law Commission of India, *supra* note 735, at 41.
[802] *Government plans to amend anti-dowry harassment law*, THE ECONOMIC TIMES (March 15, 2015), https://economictimes.indiatimes.com/news/politics-and-nation/government-plans-to-amend-anti-dowry-harassment-law/articleshow/46571163.cms.

by survivors to withdraw complaints and arrive at 'settlements'. In the context of the DV Act, though no official proposals for dilutions have been made yet, the situation may change in the near future. This is because of the government gradually buying into claims of misuse of the DV Act.[803]

Secondly, because of the vehement assertion of this perception, the focus of reform stays on curbing the alleged misuse. Hence, the discourse stays clear of examining ways to address the various barriers to accessing justice in domestic violence cases, as well as challenging the problematic notions regarding domestic violence that have pervaded the legal system. The judgement in *Social Action Forum* is a quintessential example of this phenomenon. In the case, the sole focus of the Supreme Court remained the alleged rampant misuse of the provisions by women, and the appropriate measures to curb such misuse. In the process, the other aspects of the prayer of the lead petitioner, focussing on the implementation of measures to make the legal system more accessible for women, remained unaddressed.

Hence, in various ways, this perception serves patriarchal interests by contributing to the maintenance of women's subordination within the family.

V. CONCLUSION

The perception that domestic violence provisions have been significantly misused by women has been a constant in many domestic

[803] *Domestic Violence Act misused: Centre*, THE HINDU (May 12, 2016), https://www.thehindu.com/news/national/domestic-violence-act-misused-centre/articl e8586646.ece.

violence judgements. The same has significantly influenced the dilution of the procedural rules to be followed in such cases, and judges' decisions in domestic violence cases. However, an analysis of the grounds for this perception reveals that the same is based on an ignorance of the social and practical barriers faced by women in pursuing domestic violence cases. Further, judges cite high acquittal rates as pointing to the rampant misuse of the provisions, specifically Section 498A. They hence fail to recognise the various social and legal factors that influence the high acquittal rates in such cases. This perception of rampant misuse has persisted in part because it stems from and reinforces the patriarchal values and norms deeply embedded in the Indian social structure. Further, over time, it has served various patriarchal ends by playing a significant role in turning the clock back on the legal protections available to women.

Such a perception must not influence adjudication. To this end, all the judgements that have affirmed and sought to prevent this rampant misuse must be overruled to that extent. For example, the guidelines diluting the procedure in Section 498A cases that were laid down in *Rajesh Sharma* based on this perception, and upheld in *Social Action Forum*, must be overruled. Concomitantly, there needs to be a comprehensive examination of the tenability of the various other judicial perceptions relating to domestic violence as well, such as instances of violence being transient issues best settled through reconciliation. Thus, there is a need for the explicit recognition of the misperception on part of the judges that domestic violence provisions are subject to misuse by women and their relatives, which would, in turn, increase the efficacy of legal provisions

concerning domestic violence, and would help reduce the barriers in access to justice for victims.

NLUJ Law Review

Dipti Lavya Swain, *Unpacking the Pre-Pack – A Fresh Insolvency Resolution Process Arrives in India*, 8(1) NLUJ L. REV. 217 (2021).

UNPACKING THE PRE-PACK – A FRESH INSOLVENCY RESOLUTION PROCESS ARRIVES IN INDIA

*Dipti Lavya Swain**

ABSTRACT

The recent amendment of the Insolvency and Bankruptcy Code, 2016, that was promulgated by the President of India in August 2021, is being viewed as the most prominent landmark change within the entire insolvency procedure as it has introduced a highly anticipated and wholly new scheme/procedure. The pre-packaged insolvency resolution process and the essential aims of this process are to bring in increased efficiency in terms of time, money, and cost to stakeholders, and is also a comparatively less invasive regime in aiding micro, small and medium businesses and enterprises. The following paper attempts to comprehensively discuss and elaborate on this new regime. Firstly, the author discusses the context in which such regime has been enacted, followed by a detailed comparative analysis of the existing international regimes. Furthermore, a detailed descriptive analysis of the procedure and a comparison of the new process with the older regime of Corporate Insolvency Resolution Process is undertaken. In conclusion, this paper highlights the potential challenges and issues that this new regime could face in the future.

* The author is a Partner at HSA Advocates and the Founder and Managing Partner of DLS Law Offices and may be contacted at **diptilavyaswain@gmail.com**.

TABLE OF CONTENTS

I. INTRODUCTION

The Insolvency and Bankruptcy Code, 2016 [*hereinafter* "**IBC**" or "**the Code**"] which was enacted over half a decade ago, was and continues to be a historic law that has ushered in significant changes to the nation's corporate structure. The objectives of the IBC were to regulate the relations between creditors and debtors; to make the process more efficient; and to resolve the compelling issue of growing stress assets in the country. This was followed by the period between 2008 to 2014, wherein Indian banks were lending money at high risks without due diligence. This culminated into an excessively high percentage of non-performing assets, and the IBC was finally brought in to resolve this.[804]

The IBC lays specific time bound procedures and processes as strict timelines exist for the whole Corporate Insolvency Resolution Process [*hereinafter* "**CIRP**"],[805] however, these timelines do not incorporate the time consumed by judicial or legal proceedings, and thus, practically lead to many processes exceeding the maximum number of days stated within the Code's timeline. Therefore, the most pertinent and relevant change that was required was one to tackle these issues and bring in a quick and effective resolution process, which has been brought in through the most recent amendment to the Code.

---

[804] '*12 large NPA cases listed for insolvency yet to come before IBBI*', MINT, (June 19, 2017), https://www.livemint.com/Industry/TDenpfU0nhiXjlqAE6ZtPJ/12-large-NPA-cases-listed-for-insolvency-yet-to-come-before.html.

[805] Insolvency and Bankruptcy Code, 2016, No. 31, Acts of Parliament, 2016, §33.

On 3 August 2021, the Rajya Sabha (Upper House of the Indian Parliament) passed the Insolvency and Bankruptcy Code (Amendment) Bill, 2021, which had already passed by the Lok Sabha (Lower House of the Indian Parliament) on 28 July 2021.[806] Pursuant to these legislative actions, the Insolvency and Bankruptcy Code (Amendment) Act, 2021 [*hereinafter* "**2021 Amendment**"] came into effect, however, as per Section 1(1) of the 2021 Amendment, its provisions would be deemed to have come into force with effect from 4 April 2021.

Prior to the 2021 Amendment, the Government of India had issued a notification in exercise of its powers under Sections 239(1) and 239(2)(fd) read with Section 54C(2) of the IBC as amended by the Insolvency and Bankruptcy Code (Amendment) Ordinance, 2021 (03 of 2021), thereby bringing into effect the Insolvency and Bankruptcy (Pre-packaged Insolvency Resolution Process) Rules, 2021 [*hereinafter* "**Rules**"].[807] Certain regulations[808] for the pre-pack process have also been released by the market regulator, *i.e.*, Insolvency and Bankruptcy Board of India [*hereinafter* "**IBBI**"]. The ordinance was with respect to pre-packaged insolvency resolution process [*hereinafter* "**PIRP**"] for the micro, small and medium

[806] The Insolvency And Bankruptcy Code (Amendment) Ordinance, 2021, No. 3, Acts of Parliament, 2021, https://ibbi.gov.in//uploads/legalframwork/52f66d913dfe1c637b6a38f82d38bcbd.pdf.

[807] Insolvency & Bankruptcy Board of India (Pre–Packed Insolvency Resolution Process) Rules, 2021, https://ibbi.gov.in//uploads/legalframwork/f75906d8657a51f214785c697d9bb296.pdf.

[808] Insolvency & Bankruptcy Board of India (Pre–Packed Insolvency Resolution Process) Regulations, 2021, https://ibbi.gov.in//uploads/legalframwork/2021-04-10-182311-5ngd9-0dd40b82af7a770d5e89c0d9e37bdb45.pdf.

enterprises [*hereinafter* "**MSMEs**"]. Before this, India did not have specialised norms such as the PIRP for MSMEs. However, such mechanisms have been prevalent in some western countries. In fact, in light of the ongoing COVID-19 pandemic, the World Bank and the International Monetary Fund also recommended member states to take measures to brace the inevitable impact of the pandemic on their economies.[809]

The Interim Report of the Bankruptcy Law Reform Committee [*hereinafter* "**BLRC**"] of 2015 discussed the viability of 'pre-packs' for the first time in the Indian context. The discussion was rejected considering the non-viability of out of court settlements in the Indian insolvency regime as it was then deemed to not be a wise step.[810] Owing to COVID-19, the disruption of economic processes in India led to a massive wave of insolvencies, with small businesses and industries bearing the maximum brunt owing to their size and scale. This challenge necessitated a change in India's insolvency regime, in terms of certain interim and transitional measures to flatten the curve of insolvencies and protect the small enterprises, thus leading to the current amendment.

---

[809] COVID-19 (Coronavirus) Response, The World Bank, https://www.worldbank.org/en/region/sar/coronavirus; Questions and Answers, The IMF's response to COVID-19, International Monetary Fund, https://www.imf.org/en/About/FAQ/imf-response-to-covid-19.

[810] DEPARTMENT OF ECONOMIC AFFAIRS, MINISTRY OF FINANCE INTERIM REP. OF THE BANKRUPTCY LAW REFORM COMM. (2015), https://msme.gov.in/sites/default/files/Interim_Report_BLRC.pdf.

Part II of this paper analyses and brings an international context to the pre-pack mechanism and how various jurisdictions have implemented the process, followed by Part III which briefly dwells into how MSMEs are relevant in context of PIRP. Part IV extensively and comprehensively lays down India's current PIRP process that has been brought in through the 2021 Amendment; Part V of the paper compares and juxtaposes CIRP with PIRP and analyses the same. Finally, the paper concludes with highlighting the major discussions throughout the paper and analyses the potential challenges and issues that this process might face.

II. COMPARATIVE ANALYSIS WITH INTERNATIONAL MARKETS AND JURISDICTIONS

In this section, legal provisions of countries such as the United Kingdom [*hereinafter* "**UK**"], the United States of America [*hereinafter* "**USA**"], Canada, South Korea and Singapore will be discussed which would aid in contextualising the PIRP. Historically, in the USA, the PIRP mechanism has existed following its Bankruptcy Reform Act of 1978[811] due to rapid growth of its debt-equity practice. According to a research, about 20% of all public bankruptcy in the USA had been pre-packaged by the end of the 19th century.[812] PIRP has thereafter been embraced by many countries such as France, Netherlands, Germany, South Korea, Singapore and the

[811] United States Bankruptcy Act, 11 U.S.C. § 101(1978).
[812] *Vanessa Finch*, CORPORATE INSOLVENCY LAW PERSPECTIVES AND PRINCIPLES 454 (2nd ed. 2009).

UK.[813] Pre-packs are referred to as 'expedited reorganisation proceedings' by the United Nations Commission on International Trade Law [*hereinafter* "**UNCITRAL**"][814], with the rationale that they are a combination of voluntary restructuring negotiations in which the plan is negotiated and agreed upon by all relevant parties and stakeholders, as well as a reorganised process or proceeding that begins almost immediately and without delay.

Although the market and the legal system in the UK have embraced the pre-pack process and its evolution, the applicable laws, the Insolvency Act of 1986[815], did not specifically identify or provide for a managed pre-pack procedure. The process evolved within the UK via commercial practices and business innovations. The administrator in the UK is comparable to the Interim Resolution Professional [*hereinafter* "**IRP**"] in India. Now, thanks to the Enterprise Act of 2002[816], the process of appointing an administrator without a court referral is legal. The administrator is bound and limited by the Statements of Insolvency Practice [*hereinafter* "**SIP**"], as well as the requirement of being a licenced insolvency practitioner.

The main problem raised earlier was the ethical nature of these pre-pack processes and how they are administered, as well as how to cope with

---

[813] *Bo Xie*, COMPARATIVE INSOLVENCY LAW: THE PRE-PACK APPROACH IN CORPORATE RESCUE (2016).
[814] UNCITRAL, LEGISLATIVE GUIDE ON INSOLVENCY LAW 25 ¶ 16 (2005), https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/05-80722_ebook.pdf.
[815] Insolvency Act, 1986 c. 45.
[816] Enterprise Act, 2002 c. 40.

these difficulties. SIP 16 was published in 2009, and it addressed a number of issues, including: clarifying the relationship between the administrator and the directors of the insolvent company before the administration; and stating that the administrator is only concerned with and acting in the interests of the company, not individual directors. According to SIP 16, the administrator should also assure the creditors that he would act in their best interests. SIP 16 was later amended post recommendations from a committee set up to deal with issues on sale of assets and connected party pre-packs; the amendments increased the transparency within the pre-packs to resolve those concerns and issues.[817] The changes in governance have been increasingly made as recently as 2020. New legislations were also enacted which introduced provisions allowing pre-pack processes or transactions to related parties to be examined, thus aiding in resolving the negative aspects that were caused due to the pandemic wherein extensive use of the pre-pack mechanism was being made.[818] The UK's practice which started through commercial and market aspects, wherein informal agreements were being done, has now progressively turned into a more governed process to resolve the issues that couldn't be relieved through informal means.

[817] Statement of Insolvency Practice (SIP) 16 - Background and Key Amendments, (2015), https://www.icaew.com/-/media/corporate/files/technical/insolvency/regulations and standards/sips/england/sip-16-e-and-w-pre-packaged-sales-in-administrations-2015.ashx.

[818] INSOLVENCY SERVICE (OF UK), PRE-PACK SALES IN ADMINISTRATION REP. (2020), https://www.gov.uk/government/publications/pre-pack-sales-in-administration/pre-pack-sales-in-administration-report.

In the USA, pre-packaged bankruptcy and insolvency procedures along with previously ordered bankruptcy procedures have been clearly explained and set forth in Chapter 11 of the US Bankruptcy Code[819] [*hereinafter* "**US Code**"]. Section 363 of the US Code deliberates upon the permission to carry out both of these proceedings.[820] In the USA, a process known as a pre-plan transaction entails getting rid of all corporate debtor's [*hereinafter* "**CD**"] assets until the entire restructuring process or reorganisation begins. Second, since Chapter 11 also states that the CD will inform or notify all parties involved in the proceeding and give them the opportunity to appeal if they have problems with the ongoing process or the settlement, the CD essentially needs to obtain court approval. As far as legislative involvement is concerned with these pre-planned transactions, there exists no specification with regards to any necessities or criteria that are relevant for judicially assessing the transactions or even how the same needs to be done or conducted. In simple terms, in a typical pre-planned or pre-packaged bankruptcy case, the CD and the core creditors get into a negotiation to plan out the terms of the proposal and then those negotiated proposals need approval or a 'no-objection certificate' from the separate group of creditors. Thereafter, the CD distributes the final plan to all the creditors with a disclosure statement, and then the final petition under Chapter 11 of the US Code after getting all the necessary approvals and votes in favour of the process is filed.[821]

---

[819] United States Bankruptcy Code, 11 U.S.C. (1978).
[820] *Id.*
[821] *Id.*

When a business is in debt in Canada, a ready-made sale of that business by company management often occurs as if the business is going through a difficult and worrying time looking for potential buyers. Company management under the Companies' Creditors Arrangement Act [*hereinafter* "**CCAA**"][822] seeks coverage to allow them time and money to resume their efforts to finalize the sale of the company with an eligible buyer.

In South Korea, the relevant legislation is the Debtor Rehabilitation and Bankruptcy Act, 2005,[823] which contains the procedural blueprint of restructuring plans already drawn up, and although it was introduced much later than in the UK or the USA, it has shown to be an important and effective tool to shorten the total duration of the bankruptcy procedure in the country. The intent behind the inclusion was that it would be widely used by any indebted business or corporation in dire need of an efficient path of restructuring and sustainability, and fortunately for the lawmakers, their efforts have been fruitful. Even the South Korean court system is working to take drastic and progressive measures to increase a significant proportion of pre-designed restraining procedures or agreements in order to effectively achieve the original goal.

Under Section 211 of the Singapore Companies Act,[824] the court has the power to approve a compromise or agreement between the

---

[822] Companies' Creditors Arrangement Act, R.S.C, 1985, c. C-36.
[823] Debtor Rehabilitation and Bankruptcy Act, (S. Kor.), (No. 7428 of 2005) *translated in* Korea Legislation Research Institute's online database, https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=46315&type=new&key=.
[824] Companies Act, (No. 42 of 1967) (Sing.).

corporate parties and a conference of creditors or group of creditors. If approved, this agreement will be applicable and binding on all parties, and the corporations or the various classes of creditors that are part of this agreement or are regulated by it. However, due to the pandemic, a new amendment law called the Insolvency, Restructuring and Dissolution (Amendment) Act, 2020[825] was passed in the Parliament of Singapore, which introduced a new pre-packaged process within the landscape with a focus on micro and small businesses similar to India. If a company or firm goes through this process, it will be temporarily suspended. It would also not be enough to just have a meeting with the company's creditors; the court's sanction would only be achieved if the corporate could effectively show that if a committee were to be scheduled, an extensive majority of creditors, *i.e.*, two-thirds of the total, would have given approval for it.

III. WHAT IS AN MSME?

Before moving further, it would be interesting to understand what constitutes an MSME, of which, as per India Brand Equity Foundation, over 63 million exist in India,[826] with the number growing expeditiously in the wake of several benefits being introduced from time to time by the Government.

The Micro, Small and Medium Enterprises Development Act, 2005 [*hereinafter* "**MSME Act**"], adopted by the Indian government, classified

---

[825] Insolvency, Restructuring and Dissolution (Amendment) Act, (No. 39 of 2020)(Sing.).
[826] *MSME Industry in India*, INDIA BRAND EQUITY FOUNDATION (May 20, 2021), https://www.ibef.org/industry/msme.aspx#login-box.

micro, small, and medium enterprises based on two factors: (i) investment in plant and machinery, and (ii) turnover of the business.

For firms in the manufacturing and service sectors, different thresholds for being designated as an MSME were specified based on the two considerations. However, under the government's "self-reliant India" campaign, popularly known as Aatmanirbhar Bharat Abhiyan, the Ministry of MSME amended MSME categorization by introducing a composite criterion for both plant and machinery investment and yearly turnover of firms in its notice dated 1 June 2020.[827] In addition, the distinction between manufacturing and services industries in the previous MSME definition has been eliminated. This removal will bring the sectors closer together.

In PIRP, instead of a public bidding process, the resolution of a distressed company's debt is made with a direct arrangement between secured creditors and existing owners or outside investors. Financial creditors will agree to terms with the promoters or a possible investor under the PIRP procedure, and the resolution plan will be submitted to the National Company Law Tribunal [*hereinafter* "**NCLT**"] for approval.

The reasons for introduction of PIRP for MSMEs is largely based upon providing MSMEs with a chance to restructure their liabilities and start over while maintaining enough safeguards to ensure that the system is not abused by businesses to avoid making payments to creditors. However, any resolution plan that delivers less than full recovery of dues for

[827] Ministry of Micro, Small and Medium Enterprises, S.O. 1702(E) (Notified on June 01, 2020).

operational creditors is subject to a 'Swiss challenge', a method of public procurement[828], under the PIRP method.

Any third party might propose a resolution plan for the distressed company under the Swiss challenge procedure, and the original application would have to either match the improved resolution plan or forego the investment. The process as a balance between long and informal solution processes offers certain inherent advantages, some of which are: quick resolution; cost effectiveness; boasting of the value; and preservation of employment and judicial convenience, as the time and effort required before the judicial authority would be much less owing to the largely friendly and flexible nature of the procedure. Thus, the process thrives with minimal interference.

IV. INDIA'S CURRENT PRE-PACKAGED INSOLVENCY RESOLUTION PROCESS

A PIRP can essentially be understood as an 'out-of-court arrangement' between the debtor and creditors on a 'restructuring plan'. As per the Merriam-Webster Dictionary, in this form of settlement, the debtor agrees to the terms of the creditors, reducing the time it takes to handle the business at hand.[829] A pre-packaged administration has been defined in the

---

828 Pretika Khanna, *What is the Swiss Challenge Method?*, MINT, July 16, 2015, https://www.livemint.com/Politics/HOCSnmCWarO4hpYglBsHBP/What-is-the-Swiss-Challenge-Method.html.

829 *Pre-packaged bankruptcy*, Merriam-Webster.com Legal Dictionary, https://www.merriam-webster.com/legal/pre-packaged%20bankruptcy.

UK as "*an arrangement under which the sale of all or part of a company's business or assets is negotiated with a purchaser before the appointment of an administrator, and the administrator effects the sale immediately on, or shortly after, his appointment.*"[830]

This mechanism provides an opportunity for the parties to form a consensus over the future of the business of the debtor *ex-ante*, under the interest of all stakeholders. It is based on the principle of 'corporate rescue', rather than imposing punitive liability on the CD. In India, a PIRP now appears in the form of new Sections 54A to 54P under a new Chapter III-A in the IBC, according to the 2021 Amendment.

V. THE AMENDMENT OF 2021: KEY HIGHLIGHTS

Following are the key highlights of the 2021 Amendment for PIRP:[831]

A. INITIATION OF PROCESS:

A PIRP can be initiated only by the CD, unlike in the CIRP which can be filed both by the CD or the creditors.

The following criteria needs to be fulfilled by the CD to be able to file for PIRP, as required under Section 54A of the IBC (as amended by the 2021 Amendment):

---

[830] Lorraine Conway, '*Pre-pack Administrations, House of Commons Library, Briefing Paper Number CBP5035*' HOUSE OF COMMONS LIBRARY (2017), http://researchbriefings.files.parliament.uk/documents/SN05035/SN05035.pdf.

[831] The Insolvency And Bankruptcy Code (Amendment) Act, 2021, No. 26, Acts of Parliament, 2021, https://ibbi.gov.in//uploads/legalframwork/0150ec26cf05f06e66bd82b2ec4f6296.pdf.

- The CD must be following the due process of law under Section 29A of the IBC and Section 240A to be eligible to submit a resolution plan;[832]
- The CD must not be undergoing CIRP;
- No order to liquidate the concerned company of the CD should have been passed under Section 33 of the IBC;
- The cooling-off period for initiating a fresh PIRP from completion of the previous CIRP or PIRP is 3 years. Hence, the CD must not have undergone a CIRP or PIRP for three years; and
- The majority of the partners and directors of the CD must have filed a declaration under Form P6[833] as prescribed in Section 54A(2)(f) of the IBC stating that an application for initiating PIRP will be filed by the CD within 90 days of the initiation of the PIRP, and the intent of the process is not to defraud any person. It will also contain the name of the proposed Insolvency Professional to be appointed for executing the process.

B. ROLE OF THE CREDITORS:

The PIRP route for insolvency resolution has to be agreed upon by a minimum of 66% of the financial creditors, not being its related parties representing the value of the financial debt due to such creditors. They form the Committee of Creditors [*hereinafter* "**CoC**"] for this purpose and have

[832] The Insolvency and Bankruptcy Code (Amendment) Act, 2017, No. 8, Acts of Parliament, 2018.
[833] The Insolvency and Bankruptcy (Application to Adjudicating Authority) Rules, 2016, Gazette of India, pt. II sec. 4 (Nov. 30, 2021) (No. 828 of 2016).

to express their consent for initiating PIRP by passing a special resolution. Section 54A(2)(e) of the 2021 Amendment provides that in a situation where the CD does not have any financial creditors, not being its related parties, a proposal and approval shall be provided by such persons as may be specified.

A 'creditor', as defined by Section 3(10)[834] of the IBC, is any individual who is owed a debt, including a financial creditor, an operational creditor, a secured creditor, an unsecured creditor, and a decree holder.

C. FILING OF THE APPLICATION:

Once approved by the CoC, the application for PIRP has to be filed through Form P4[835] with the Adjudicating Authority, *i.e.*, the NCLT. The NCLT must approve or reject the application within fourteen days of its receipt. In case any corrections need to be made to the plan, the CD has to be given notice within seven days of applying to rectify the fault.

D. DEFAULT AMOUNT:

The 2021 Amendment has set the upper limit of the default amount at INR 1 crore (USD 134,699). Hence, PIRP can be filed when the defaulted debt ranges from INR 10 lakh (USD 13,470) to INR 1 crore (USD 134,699.70). When all the criteria are fulfilled and the Adjudicating Authority accepts the application submitted, a Resolution Professional [*hereinafter* "**RP**"] is appointed to carry out the process.

---

[834] Insolvency and Bankruptcy Code, 2016, No. 31, Acts of Parliament, 2016, §3(10).
[835] *Id.*

E. COMPANY MANAGEMENT:

The administration of the company is retained by the CD, or whoever is appointed by them on their behalf, during the process. Only in cases of the existing management being involved in fraudulent activity is the responsibility to manage the company is transferred to the RP.

F. BASE RESOLUTION PLAN:

The CD is expected to formulate a base resolution plan under Section 54K for debt restructuring and submit it to the RP within two days of the beginning of the process. The CoC may accept it or allow the CD to revise it. In case the base resolution plan is not accepted by the CoC even after revision, the RP is supposed to invite prospective resolution applicants to submit their resolution plans to compete with the base resolution plan.

G. APPROVAL BY COC:

The resolution plans which align with the requirements of Section 30(2) of the IBC are presented to the CoC by the RP. These resolution plans are then evaluated by CoC and one of them is selected under Sub-sections 10, 11 or 12 of Section 54K. It is then submitted to the Adjudicating Authority within 90 days. [836]

H. APPROVAL BY ADJUDICATING AUTHORITY:

Once the resolution plan is filed, the NCLT must approve the plan within 30 days. The entire process has to be finished within 120 days.

[836] Insolvency and Bankruptcy Code, 2016, No. 31, Acts of Parliament, 2016, §54L.

However, NCLT may not approve it and instead pass an order of termination of the PIRP on the following grounds:[837]

- a resolution plan is not submitted to the NCLT within 90 days,
- the resolution plan successful in the competition between the base resolution plan and the selected resolution plan is not approved by the CoC, or
- the CoC passes a resolution seeking termination.

In such cases, the RP is supposed to apply to the NCLT for dissolution of the PIRP.

I. POWER OF TERMINATION BY COC:

According to Section 54N(2) of the IBC, the PIRP can be terminated at any time before approval of the plan if a minimum of two-thirds of the CoC votes to terminate the PIRP. They can also vote to initiate the CIRP instead of the PIRP (in case the CD is eligible for the CIRP) before the approval of the PIRP by the NCLT. In such a situation, they must inform the RP accordingly.

J. COST EFFICIENCY:

The cost of the PIRP has been reduced when compared to the hefty money otherwise required for carrying out the CIRP. It is due to the voluntary form of restructuring with more involvement from the stakeholders that all unnecessary litigations, costs and delays can be avoided.

---

[837] Insolvency and Bankruptcy Code, 2016, No. 31, Acts of Parliament, 2016, §54L(3).

The Memorandum Regarding Delegated Legislation of the 2021 Amendment empowers the Central Government and the IBBI to make and amend the rules in respect of matters relating to forms, costs, conditions and restrictions on discharging of the rights of the involved parties.

VI. COMPARATIVE ANALYSIS OF CIRP AND PIRP

The CIRP's main flaw is that it takes an inordinate amount of time to resolve. By the end of March 2021, 79 percent of the 1,723 insolvency resolution proceedings in progress had passed the 270-day mark. This can be attributed to the prolonged litigation by the creditors and shareholders, as well as the practice of virtual hearings in the current scenario. In contrast, the PIRP is limited to a maximum of 120 days with 90 days available to stakeholders to bring a resolution plan for approval before the NCLT.[838] The minimum threshold amount for initiating a PIRP should be between INR 10 Lakh to INR 1 Crore, while the same starts at INR 1 Crore for a CIRP.[839]

While CIRP requires a mandatory involvement of the Adjudicating Authority at all stages, PIRP requires the consent of both the parties to initiate the process and only involves the NCLT in the final stage of submitting the base resolution plan, and hence has a limited role for the Adjudicating Authority to play.[840] A PIRP is hybrid in its approach as it gives space to the CD and financial creditors to come on mutually agreeable

[838] Insolvency and Bankruptcy Code, 2016, No. 31, Acts of Parliament, 2016, §54D(1).
[839] MCA Notification, *supra* note 808.
[840] Insolvency and Bankruptcy Code, 2016, No. 31, Acts of Parliament, 2016, §54D(1).

terms for restructuring of the company, as well as necessitates the intervention of the Adjudicating Authority to implement the plan.

In general, the PIRP provides more freedom and choice to the debtors in terms of making their restructuring plan and further allows making amendments to it based on the recommendations of the CoC. Another significant distinction between the PIRP and CIRP is that in PIRP, existing management keeps control; in CIRP, a RP assumes control of the debtor as a representative of financial creditors. As a result, a PIRP is significantly less disruptive to the business in question. At the same time, a PIRP can only be started by the CD, whereas a CIRP can be started by both the creditors and the debtor.

VII. CONCLUSION

It has been realized through the journey of the PIRP in various other jurisdictions that it is an effective mechanism for a speedy resolution. However, there are also certain challenges in its operation. The first issue is that due diligence may be overlooked in light of the quick completion of the resolution process. If suppliers believe the proper procedure was not followed, the company's reputation may be harmed, and this will cause additional problems if the company is later sold to a third party. Because the court's involvement is minimal, creditors have been known to later claim that their interests were disregarded (since the consent of only 66 percent of financial creditors needs to be taken). Unsecured creditors, in particular, are frequently kept in the dark until the procedure is over, thus making them feel alienated throughout the process.

There is also a concern that since the process is normally confidential and only receives the consent of secured creditors, there is insufficient incentive to conduct extensive marketing that is in the interest of all creditors, especially unsecured ones. Given this, the value due to unsecured creditors may be captured by other stakeholders.[841] There have also been some instances where pre-packages have been used by related parties where the company is only technical and not bankrupt to profit from balance sheet reshuffle, especially to undermine its business competitors.

Under the current Indian regime of IBC, insolvency professionals are still developing the necessary expertise required with time. Just as the law under the UK regime has evolved, the application of pre-packaged insolvency in India will require a much higher degree of expertise of insolvency professionals. In addition, creditors must build trust not only in these liquidators/insolvency professionals, but also in the framework created so that there is an understanding between creditors when negotiating and approving plans. At the same time, CDs must be aware of their worth as they have to identify and execute plans that are fair and reasonable for all. A sense of cooperation between both these parties is of paramount significance as an out-of-court debt restructuring arrangement can only be possible in a scenario where both parties are willing to negotiate.

The key features of the PIRP in the 2021 Amendment have been designed to play an instrumental role in saving the distressed MSMEs from

---

[841] Sandra Frisby, *A Preliminary Analysis Of Pre-Packaged Administrations*, III GLOBAL (2007), https://www.iiiglobal.org/sites/default/files/sandrafrisbyprelim.pdf.

going through complete liquidation and bankruptcy, and hence, will hopefully provide them with respite. The revised definition of the MSME sector covers almost 70% of the Indian industries. At the same time, the Supreme Court of India has held in the very recent case of *Silpi Industries* v. *Kerala SRTC*[842] that to seek the benefit of provisions under MSME Act, the seller should have registered under the provisions of the Act, as on the date of entering into the contract. In any event, for the supplies pursuant to the contract made before the registration of the unit under provisions of the MSME Act, no benefit can be sought by such entity, as contemplated under MSME Act.[843] With 90% of MSMEs being unregistered, the judgement can potentially exclude a majority of the MSMEs in India to be eligible to apply for PIRP, hence, this is a challenge that needs to be resolved immediately for effective implementation of the 2021 Amendment.

Recently, the IBBI stated that based on the experience of PIRP for MSMEs, there is a possibility that the scheme will be extended to large companies as well in the future.[844] With the rise of out-of-court settlements, PIRP may become a viable option to CIRP in the near future. However, considering the quantum of such matters in the country, each law and novice system will need to undergo the rigours of such process and pass

---

[842] Silpi Industries v. Kerala SRTC, 2021 SCC OnLine SC 439.

[843] Tariq Khan, *Pre-Packs for MSMEs: A Positive Step with Implementation Hurdles,* SCC ONLINE (July 20, 2021), https://www.scconline.com/blog/post/2021/07/20/pre-packs-for-msmes-a-positive-step-with-implementation-hurdles/.

[844] Banikinkar Pattanayak, *IBBI hints at Pre-pack scheme for large firms*, FINANCIAL EXPRESS (Aug. 3, 2021), https://www.financialexpress.com/industry/ibbi-hints-at-pre-pack-scheme-for-large-firms/2302882.

the test of time, to finally decide as to whether or not such a change was indeed useful and worthy.