THE CRIMINAL LAW REVIEW

VOLUME 9 NO. 1
2023 (75 RR)

SARDAR VALLABHBHAI PATEL NATIONAL POLICE ACADEMY
HYDERABAD

SVP National Police Academy

Criminal Law Review-2023(75RR)

Volume - 9 No. 1

Published by

SVP National Police Academy
Hyderabad

SVP NPA Criminal Law Review 2023

ADVISORY COUNCIL

Shri Amit Garg
Director
SVP NPA

Editor:
Dr. Rohini Katoch Sepat
Deputy Director (IS I)
&
Faculty Counsellor
Law Society, SVP NPA

Ms. Isha Singh
(75 RR – AGMUT Cadre)
Secretary
Law Society, SVP NPA

Advisor:
Dr. Anju Choudhary
Ex-Faculty, SVP NPA

Vol. 9 No.1 2023

Ms. Sudhanshu Nayak

Ms. Suman Nala

Mr. Tarun Goyal

Mr. Vagisha Joshi

Mr. Vedant Shankar

Mr. Vimal Kumar Pathak

NPA Criminal Law Review

Vol. 9	No.1	2023

CONTENTS

सरदार वल्लभभाई पटेल राष्ट्रीय पुलिस अकादमी
(गृह मंत्रालय भारत सरकार)
हैदराबाद - ५०००५२
SARDAR VALLABHBHAI PATEL NATIONAL POLICE ACADEMY
(*Ministry of Home Affairs, Government of India*)
HYDERABAD - 500052

AMIT GARG, IPS
I/c. DIRECTOR

FOREWORD

Knowledge of Criminal Law and Procedure is the cornerstone of policing. In an age when transparency is the buzz word, adherence to the Law is absolutely essential. The curriculum at the Sardar Vallabhbhai Patel National Police Academy strives to inculcate a deeper interest, among the Trainees, in the study of Law.

The NPA Criminal Law Review is a commendable step in this direction. It comprises contributions from authors ranging from the Faculty of the Academy to the IPS Officer Trainees of the 75 RR. The articles are thought provoking and should be of interest to police officers, lawyers and academicians alike. I am hopeful that this publication will kindle an aptitude for research among the leaders and will encourage others to contribute.

I congratulate the members of the Law Society for this compilation and wish them a bright and successful career.

Dt.23.10.2023

(Amit Garg)

E Mail : info@svpnpa.gov.in Tel : 040-24015151-58, PRI No: 040-24235999 Fax: 040-24015179

Sardar Vallabhbhai Patel
National Police Academy
Criminal Law Review 1-9

A Proactive Future: Cybersecurity in a Digital Age

ISHA SINGH *

"The greatest victory is that which requires no battle."

— Sun Tzu, The Art of War

From the digitalisation of basic tasks such as domestic work to enhanced communication through social media to high level technological advances such as quantum computing, cyberspace pervades every part of our existence. There's no escaping the digital present and future that stares us in the face. India, with a burgeoning population of 1.3 billion people, with 692 million active internet users, estimated to be 900 million by 2025, will do well to recognise that if not anticipated and regulated, the internet can turn into an uncontrollable Leviathan for the State.

India's Scourge: A Tradition of Reaction

The fundamental shortcoming in the entire policy design of cyberspace regulation in India is its reactive approach. The Information Technology Act was passed in 2000 ("IT Act"), well after Prime Minister Rajiv Gandhi's 1984 plan for the large-scale adoption of computers in 1984. The objective behind this enactment was the

* *IPS (Probationer) 75 RR, AGMUT Cadre*

regulation of electronic commerce, with negligible focus on cybercrime and cybersecurity. The criminal offences were delineated under Sections 65, 66 and 67. This must be contrasted with the United States' Computer Fraud and Abuse Act of 1986 ("CFAA") and Computer Security Act of 1987 ("CSA"). These legislations were passed in response, but also in anticipation of the growing expanse of the cyber world and the accompanying challenges. For instance, the CFAA criminalised "unauthorised access" of computers, computer espionage and damaging a protected computer in 1986 itself. Till date, cyber espionage is not a specific offence under the IT Act, allowing multiple perpetrators to go unchecked.

The CSA too was a futuristic legislation, which focused on enhancing the security and privacy of sensitive information, minimal acceptable security practices and empowering the National Institute of Standards and Technology ("NIST") for the creation of cybersecurity plans in consultation with the National Security Agency. This enabled the US to gain a first mover advantage in the field of cybersecurity, enabling it to shape the field, encouraging the proliferation of private players and tackling hindrances to the Silicon Valley boom. The NIST Framework is one such outcome of the Act which acts as an exhaustive guide to protecting critical infrastructure in the US.

The United Kingdom followed suit with the enactment of the Computer Misuse Act of 1990. This legislation criminalised unauthorised access of computers as well as unauthorised access with intent to commit further offences. Most interestingly, in a similar vein as the CFAA, the UK gave itself extra-territorial jurisdiction by way of Section 4 of the Act. It is pertinent to note that this extra-territorial jurisdiction is much broader in its application vis-a-vis the extra-territorial jurisdiction under the IT Act.

India on the other hand, allowed the field to remain unregulated, relying on pre-existing laws like the Indian Penal Code,

1860 and the Indian Telegraph Act, 1885 to furnish the gaps. While this legal lacuna could have been intentional, as a bid to create minimum hindrances in the adoption of technology, it gave a free reign to the nefarious elements of cyberspace. After the 26/11 attacks, through a knee-jerk reaction, the 2008 Amendment to the IT Act was passed, with minimal discussion.

Through the 2008 Amendment, unauthorised access under Section 43 was criminalised if done with a dishonest or fraudulent intention, and new offences such as identity theft, cheating by personation and violation of privacy. While this was a welcome change, due to limited deliberation, the offences remain vague and generic, resulting in over broad interpretations and criminalisation. A case in point is the *Shreya Singhal* judgement which struck down Section 66A of the IT Act. Due to ad-hocism in legislation making, over broad terms like "inconvenience", "annoyance", FIRs were being filed left, right and centre, resulting in overcriminalization.

Reassessing the Offences under IT Act

From the above, it becomes imperative to be specific in classification of offences under the IT Act and to delineate more offences. The scope of cyberterrorism under Section 66F must be expanded to include offences against private property, 'virtual property', as well as cyber espionage. The US government's response in the 2014 Sony Pictures hack must be studied to understand how a cyberattack on a private company by another country's government may be classified as a 'national security matter'. Exhaustive protocols which need to be followed in cases of cyber warfare must be notified under the Act. Reference can be made to the CFAA and the NIST Framework on Cybersecurity in this regard.

Offences must also be drafted in a specific, coherent and logical manner to avoid being struck down as unconstitutional and be

more efficient in operation. American constitutional jurisprudence has put forth the 'void for vagueness doctrine'. As per this doctrine, *"men of common intelligence cannot be required to guess at the meaning of [an] enactment."* This is particularly true of penal statutes which impinge on the liberty of citizens and thus should not leave any scope for speculation. This doctrine has been kept in mind while interpreting the CFAA in the US, and this jurisprudence was also invoked in the *Shreya Singhal* judgement. Moreover, the striking down of Section 66A due to its over broadness has had significant repercussions on law enforcement. There is no avenue to check hate speech, cyber bullying, cyber stalking and other cyber conduct which has the potential to be classified as criminal. Emerging threats through AI, quantum computing, cryptocurrency as well as Advanced Persistent Threats need to be identified, comprehensively evaluated and specifically mentioned in criminal statutes.

Thus, reference can be made to desirable drafting practices which prevail in the US, UK and Australia in order to criminalise cyber offences. Due care must be taken to avoid overlap between offences under the IPC, IT Act and the UAPA to avoid confusion in investigation and later judicial challenges and acquittals, as witnessed in the *Sharat Babu Digumarti* case. Germany's solution to this has been incorporation of cyber offences in the German Criminal Code itself. This has effectively avoided overlap and multiplicity of laws. Simultaneously, a balance must be struck, by allowing enough scope for creative judicial interpretation, given the constantly evolving domain of cyberspace. For instance, in the field of takedown of content, Germany has relied on the Bundesgerichtshof's decisions rather than Parliamentary statutes. This has provided sufficient flexibility, enabling the law to keep up with technological evolution.

Checking Digital Monopolies: The Rise of Private Bureaucracies

One of the greatest challenges facing governments today is the regulation of internet intermediaries, particularly social media companies. In part, this is attributable to the popularity of the self-regulation theory. This perspective argued that the internet was fit to govern itself and the absence of government intervention would not result in cyber anarchy. However, it was unable to anticipate the rise of cyber monopolies like Facebook, Google and Amazon, to name a few. The recent examples of Whatsapp rolling out its updated privacy policy which threatened the privacy of Indian users inspite of protests by the Indian government. Australia too faced Facebook's behemothic onslaught when the latter suspended all news on its platform in Australia to protest the News Media and Digital Platforms Mandatory Bargaining Code. Australia was forced to withdraw it due to the chaos that resulted from such a move.

The non-cooperation of digital intermediaries with governments can directly undermine national sovereignty and cause significant harm to public order. For instance, social media has steeply hiked the availability of fake news, rumour mongering, inflammatory content, troll armies, cyber bullying and the veil of anonymity, resulting in riots, mob lynchings, COVID-19 panic, and a host of other problems. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 are a step in the right direction, but insufficient to combat the gravity of the problem. Moreover, given the delicate issues at stake, fundamental rights of citizens, freedom of businesses and the safety of the nation and its people, it is imperative that a Parliamentary statute to deal with online safety be evolved, after due deliberation with relevant stakeholders.

The example of Australia's Online Safety Act of 2021 is relevant here. The Act comprehensively deals with various aspects of

cyber safety. The fact that it has Parliamentary backing accords it greater legitimacy, dissuading Courts from unduly challenging its Constitutionality. The Act deals with cyber bullying of children and adults, non-consensual sharing of images, takedown of content, removal of apps as well as basic online safety expectations and setting industry standards in this regard. It provides for criminal as well as civil penalties, making its implementation more effective and avoiding overcriminalization. India would do well to examine this and similar statutes in other jurisdictions to draw inspiration for its own.

At this point, it's also necessary to state the loss of huge revenues due to tax evasion and offshore data centres of digital monopolies. This leads to huge loss of rightful revenue and profits to the exchequer, and endangers the privacy of Indian citizens, increasing the vulnerabilities of the nation. Issues of cybersecurity breach the traditional dichotomy of civil and criminal laws. Thus, antitrust measures, tax levies, data protection laws, cyberspace regulation and cybercrime categorisation cannot operate in silos, but rather must be seen as constituent parts of a larger whole. Strategies to deal with them must be evolved accordingly.

Balancing the Rights of the People: Enacting A Digital Constitution

As recognised by the Supreme Court in *Anuradha Bhasin* v. *Union of India*, the internet has become an integral part of the everyday existence of the people. Professor Jack M. Balkin of Yale University argues that the internet must be considered akin to a public place, given the vast exercise of fundamental rights of individuals through this medium. There is truth to this statement, given that the organisation of public protests, interaction with public representatives, accessing government services like Aadhaar, enrolment in the voters list and even COVID vaccination, is done through the internet today. This rationale drove the Supreme Court to uphold access to

information through the internet as a fundamental right. Thus, citizens become important stakeholders in any form of cybersecurity intervention undertaken by the State, as well as internet intermediaries.

He further expounds that the exercise of many fundamental rights, particularly free speech, are no longer a two way relationship between the State and individuals. Rather, internet intermediaries, like internet service providers, social media companies and digital platforms play an essential role in enabling and upholding fundamental freedoms. The exercise of functions like content moderation and takedown can impinge on these freedoms. Moreover, the State lacks the technical capacity to regulate these platforms. Thus, many roles within the traditional domain of the State are outsourced to private companies, resulting in the rise of "private bureaucracies". Legislations like Germany's NetzDG Act, which combats fake news, misinformation and hate speech, and European Union's General Data Protection Regulation bank on the capacity of private companies, rather than the State, to counter cyber threats.

In light of this, it would do well to improve transparency in the regulation of the internet. This would also prompt internet intermediaries to follow suit. For instance, in spite of having the highest number of internet shutdowns in the world, India does not have a Parliamentary law on the same. This also adversely affects the Government's vision of Digital India and Atmanirbhar Bharat. Similarly, the procedure for takedown of content under the Blocking Rules of 2011 are strictly confidential. This eventually results in long drawn court battles and dwindles trust between the State and the people. Cybersecurity requires coordination of all stakeholders. Polyvocal internet governance will do wonders for enhancing cyber preparedness of the nation. Thus, proactive measures must be taken to create a collaborative approach. improve communication, information

sharing and transparency, between the State, the people and internet intermediaries.

The Vidhi Centre for Legal Policy has advocated the enactment of a digital Constitution to clarify the bare minimum framework of human rights law which will be applicable in all cases of cyber interventions and statutes. Since it is next to impossible to legislate an overarching Statute to counter the challenges of cyberspace, cyber laws are bound to be fragmented. However, a Digital Constitution can pave the way for delineating roles and understanding between all the relevant stakeholders. Reference must be made to the African Declaration on Internet Rights and Freedoms. This Declaration lays down the key principles which will guide any policy towards cyberspace. These include openness, internet access and affordability, freedom of expression, privacy and personal data protection and gender equality *inter alia.*

Embracing A Proactive Approach: Taking Indian Cyber Power to New Heights

As has been witnessed in the case of China's strategic rise, strong offensive capabilities serve as the best defence. To bolster our cyber capabilities, we must do away with a reactive response. Till date, we lack a coordinated, well-thought out vision and strategy towards cyber space. Our National Cyber Security Strategy does not account for our dreams, hopes and aspirations. This is in stark contrast to the United Kingdom's Strategy, which encapsulates its vision to become a "Cyber Power" and charts out a strategy to achieve its goals, along with delineating cybersecurity responses. Singapore is another example of a nation which has thrived with a proactive approach. It advocates active defence strategies to tackle 'Advanced Persistent Threats' through the training of cyber security experts and assessing cyber security risks. The US has established an Internet Policy Task Force under its Department of Commerce, which identifies the "nexus

between privacy policy, copyright, global free flow of information, cybersecurity, and innovation in the Internet economy". India too needs to create a policy think tank, alternatively rationalise the existing ones, which can comprehensively focus on the cyberspace domain to anticipate changes and challenges. Some researchers have suggested the use of proactive strategies like "hacking back" and "honeypots" to deter hackers.

Finally, India must consider broadening its jurisdiction under cyber laws like the US, UK and Germany have done under their respective legislations, as mentioned above. This must be coupled with multilateral cooperation with nation-states and information sharing through agencies like Interpol to achieve effective law enforcement in the field of cybersecurity.

Sardar Vallabhbhai Patel
National Police Academy
Criminal Law Review 10-21

Finding a Balance between the Argumentative Indian and Intolerant Indian: Navigating the Landscape of Hate Speech

VIMAL KUMAR PATHAK[1*]

Navigating the Landscape of Detrimental Discourse: Hate Speech, Speech We Hate and Dangerous Speech

According to the National Criminal Records Bureau (NCRB) data, between 2014 and 2020, cases filed under Section 153A of the Indian Penal Code (IPC) (incitement to hostility among different groups based on religion, race, place of birth, place of residence, language) increased sixfold or nearly 500%.

On 21st October 2022, a Supreme Court bench comprising of Justices K M Joseph and Hrishikesh Roy, in interim directions, directed the police chiefs of Delhi, Uttar Pradesh and Uttarakhand to take "immediate" suo-motu action against any hate speech, by lodging criminal cases without waiting for formal complaints. The court further warned authorities that "any hesitation to act in accordance

[*] *IPS (Probationer) 75 RR, Chhattisgarh Cadre*

with this direction will be viewed as contempt of court and appropriate action shall be taken against the erring officers".

The above direction to the police needs to be contextualised in the background that India does not have a formal legal framework for dealing with hate speech, nor does any Indian law define what is hate speech.

India is a vibrant democracy with a population of over 130 crores, we, as Amartya Sen argues are *Argumentative Indians*, who are now empowered with social media and with rising socio-economic status have ideas which are contesting with what traditionally was Idea of India. Thus, taking suo-moto actions on Hate Speech, seems like a herculean task, especially when the lines between *Hate Speech* and *Speech we hate* are seemingly lost in the noise of elections, interests and competitive intolerance.

This article is a humble attempt to understand how we as IPS officers can deal with the malice of Hate Speech.

Hate Speech can loosely be defined as expressions that seek to malign people or communities for their immutable characteristics such as their race, gender, ethnicity, religion, national origin, age, or disability. American scholar Caitlin Ring Carlson argues that Hate Speech is a structural phenomenon, it is used by people in power or majority to maintain and sustain their position in the social hierarchy e.g., Jewish people were referred as rats before the holocaust, Tutsis were referred as cockroaches in Rwanda by Hulus and more recently Rohingyas in Myanmar were compared to dogs by local Buddhists. This dehumanisation or animalization of minority communities were used as tools of hate speech to make the violence against them more palatable and for the majority to retain their primacy in their respective nation.

The state has the task of saving the lives of the people on the one hand and defending the right to speech on the other hand. Hate Speech makes these two tasks compete. Article 19 of the Constitution provides for freedom of speech and expression within the walls enshrined in article 19(2) of the Constitution.

Unveiling the Paradox: The Defense of All Speech, Even Hate Speech

These are several theories which argue that all kinds of speeches shall be allowed including hate speech:

Marketplace of Ideas- The marketplace of ideas is a rationale for freedom of expression based on an analogy to the economic concept of a free market. The marketplace of ideas holds that the truth will emerge from the competition of ideas in free, transparent public discourse and concludes that ideas and ideologies will be culled according to their superiority or inferiority and widespread acceptance among the population. Thus, we need all kinds of ideas, speeches, and expressions out in the public, competing, for the real truth to emerge. This theory finds support in works of philosophers like John Milton and John Stuart Mill.

Democratic Self Governance- This idea is based on the works of Alexander Meiklejohn who proposed in 1948 that to govern ourselves effectively, we need access to all kinds of information, including hate speech, myths and disinformation.

Personal Liberty- This idea comes from Thomas Emerson and proposes that for human beings to achieve their full human self, to self-actualize, to be the person that one is supposed to be, the government need not regulate free speech.

Bellwether argument- Which essentially says that we need to allow hate speech to understand how racist, communal, or homophobic our society is, so that we can take corrective measures.

Safety Valve argument- It essentially says, to vent out our frustration or display our disapproval it's better for us to be able to blow off steam through language rather than violent action.

Lack of trust on the governments to regulate hate speech- Given the nuanced approach needed to decide what is hate speech, it is possible that the government may use this as a tool to suppress dissent.

Shattering the Shield: Debunking Arguments for Unrestricted Speech

I believe that the *marketplace of ideas* theory suffers from the same ailments that have infected capitalism. It's important when we talk about the marketplace to really recognize how the information environment has changed. We are living in a post-truth era amplified by social media, examples like Covid vaccine disinformation, campaigns against climate change are some examples. There is an overflow of information and it's hard to determine what's a credible source and thus, a marketplace of ideas, seems good in theory, but we need to ask ourselves how does it work today? Who has access to the marketplace?

Money, race, religion, community, or gender makes a big difference about who has access to a marketplace of ideas; in terms of being able to get their message across.

Coming to democratic *self-governance*, given the amount of our civic life that we live out online, which is filled with cacophony of noise including hate speech, it's really hard to, especially for people against whom the hate speech is directed, to participate in those

debates. Thus, in this way, they are kept at the margins of processes of self-governance.

Personal liberty though important, must not damage human dignity, also personal liberty provided in the constitution is not absolute.

Hate speech negates human dignity, causes psychological, physiological & emotional harm, has a silencing effect, and creates an environment for discrimination.

These arguments clearly establish the need for regulating hate speech to establish effective governance, ensure equitable participation and to expand social freedoms.

Now, the point to ponder is how to do it? What legal provisions exist in India for the same? What is needed?

Unveiling Hate's Disguise: Hate Speech Sleuth

UN Strategy and Plan of Action on Hate Speech defines hate speech as "any kind of communication in speech, writing or behaviour, that attacks or uses pejorative or discriminatory language with reference to a person or a group on the basis of who they are, in other words, based on their religion, ethnicity, nationality, race, colour, descent, gender or other identity factor."

However, to date there is no universal definition of hate speech under international human rights law. However, hate speech has three important attributes:

1. Hate speech can be conveyed through any form of expression, including images, cartoons, memes, objects, gestures and symbols and it can be disseminated offline or online.

2. Hate speech is "discriminatory" (biassed, bigoted or intolerant) or "pejorative" (prejudiced, contemptuous or demeaning) of an individual or group.
3. Hate speech calls out real or perceived "identity factors" of an individual or a group, including: "religion, ethnicity, nationality, race, colour, descent, gender," but also characteristics such as language, economic or social origin, disability, health status, or sexual orientation, among many others.

Shades of Grey: Distinguishing between Hate Speech and Dangerous Speech

Susan Benesch calls for the need to create a distinction between hate speech and dangerous speech. Hate speech is critical of a particular faith, idea, religion, caste and race, among other identifiers. Dangerous speech takes it a notch higher, by inciting and promoting violence based on the generalisation of hate speech. There is an element of clear and imminent violence against a particular community in dangerous speech. Unless there is a direct provocation of violence or imminent fear, it is hateful speech.

There are the 6 ingredients of dangerous speech:

1. The speaker is an influential orator who is popular amongst the people he is addressing.
2. The audience is susceptible to being swayed easily.
3. The speech provokes violence against a particular community and instils fear.
4. The speech is based on a grievance or a sense of loss (typically of pride or rights) that the audience can relate to.

5. The speech touches upon the concept of purity (typically ethnic or racial) and the idea of outsiders disturbing the balance of society; and
6. The speech uses coded language to communicate an idea or dehumanise the 'other' community.

Unmasking the Viral Verbal Venom: Combating Hate Speech in the Digital Age

The growth of hateful content online has been coupled with the rise of easily shareable disinformation enabled by digital tools. Unlike in traditional media, online hate speech can be produced and shared easily, at low cost and anonymously. This raises unprecedented challenges for our societies as governments struggle to enforce national laws in the virtual world's scale and speed. However, their efforts seem insufficient owing to the sheer scale of the phenomenon, the technological limitations of automated monitoring systems and the lack of transparency of online companies.

Tarleton Gillespie in his book, "*Custodians of the Internet*" identified three tools for content moderation on social media. *Policies*- what kind of content will not be allowed on their platform, *artificial intelligence (AI)* – by using Natural Language Processing (NLP) to cull out hate speech, and *community flagging*.

However, hate speeches keep many users engaged on the social media platforms longer, thus, it goes against the business model of these companies to regulate or reduce hate speech.

Caitlin Ring Carlson in her *book Hate Speech* have suggested several measures to regulate and reduce hate speech online, these includes:

a. ***De-platforming***- which essentially involves banning the user from the social media platform and suspending his or her account. Twitter did this with former US President, Donald Trump
b. ***Shadow banning***- under this the accounts are not removed, but the social media companies are limits the reach of their content, so it's not reaching the audience which the user intended to reach
c. ***Reconsidering user anonymity*** on social media platforms
d. Mandating the social media companies to openly declare the policies followed for content moderation and how AI is being used to regulate hate speech.
e. Making social media platforms to publish *quarterly transparency reports* on how they dealt with hate speech on their platform.

In India, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, provides for regulation of social media and digital media platforms. It mandates social media companies to remove or disable access to content deemed illegal under Indian law within 36 hours and provides for appointment of grievance officers, a nodal officer, and a compliance officer for ensuring compliance with these rules.

Section 69A of the IT Act empowers the central government to direct the intermediaries to block or take down harmful content for regulating the circulation of online hate speech.

Legal Labyrinths: Navigating Indian Jurisprudence on Hate Speech

Following set of provisions of the Indian Penal Code (IPC), loosely defining hate speech, are usually invoked to deal with offences against religions.

Section 295A of the IPC: It defines and prescribes a punishment for deliberate and malicious acts, intended to outrage religious feelings of any class by insulting its religion or religious beliefs it says, "Whoever, with deliberate and malicious intention of outraging the religious feelings of any class of citizens of India by words, either spoken or written, or by signs or by visible representations or otherwise, insults or attempts to insult the religion or the religious beliefs of that class, shall be punished with imprisonment of either description for a term which may extend to [three years], or with fine, or with both".

Section 295A is one of the main provisions in the IPC chapter to penalise religious offences. The chapter includes offences to penalise damage or defilement of a place of worship with intent to insult the religion (*Section 295)*; trespassing in a place of sepulchre *(Section 297)*; uttering, words, etc, with deliberate intent to wound the religious feelings of any person *(Section 298)*; and disturbing a religious assembly *(Section 296)*.

The state often invokes Section 295A along with *Section 153A*, which penalises promoting enmity between different groups on grounds of religion, race, place of birth, residence, language, etc, and doing acts prejudicial to maintenance of harmony and *Section 505* of the IPC that punishes statements conducing to public mischief.

Section 3(1)(x) of the Atrocities Act of The Scheduled Castes and Scheduled Tribes (Prevention of Atrocities) Act, 1989 criminalises certain kinds of speech that are considered harmful to the dignity of marginalised groups, that the Atrocities Act is meant to protect.

Customs act 1962 lays down rules and regulations that permit the Central Government to prohibit the export or import of goods of specified description for purposes specified in the Customs Act.

Section 11(2)(b) of the act was most famously invoked in 1988 to prohibit the import of Satanic Verses, Salman Rushdie's controversial novel. Section 11(2) lists the purposes for which import may be banned. Among these purposes is Section 11(2)(b) the 'maintenance of public order and standards of decency or morality'.

The Religious Institutions (Prevention of Misuse) Act, 1988 was enacted to prevent the misuse of religious institutions for political and other purposes. The Act proscribes religious institutions from promoting disharmony, enmity, hatred or ill-will between various classes of people. This Act has been invoked in instances where religious institutions have been used to propagate hate speech.

Inside the Halls of Justice: A Supreme Court Insight

The Supreme Court in *Amish Devgan v. Union of India* case, referred to an article which outlined the three elements of hate speech – *content, intent, and harm or impact*. For content aspect the court re-asserted that "the effect of the words must be judged from the standards of reasonable, strong-minded, firm and courageous men, and not those of weak and vacillating minds, nor of those who scent danger in every hostile point of view"

On the intent aspect, the Court accepted the view that:

The intent-based element of 'hate speech' requires the speaker's message to intend only to promote hatred, violence or resentment against a particular class or group without communicating any legitimate message. This requires subjective intent on the part of the speaker to target the group or person associated with the class/group.
In *Amish Devgan*, the Court reaffirmed that the right to "favour or criticise" government policies is within the right to free speech, and such "political speech" does not constitute hate speech. This is an

important distinction which needs to be understood by the police. The misuse of these provisions of law to target people making political comments is illustrated in the case of *Patricia Mukhim v. State of Meghalaya*.

Silencing the Echoes of Hate: Ballot box and Hate Speech

Hate speeches during elections are dealt with by *Representation of the People's act 1951 (RoPA)*. Restrictions on hate speech are found in two distinct units of RoPA. The first is *Section 123(3A)* under Chapter I of Part VII, 'Corrupt Practices', and the second is *Section 125* under Chapter III of Part VII, 'Electoral Offences'. Electoral hate speech is one of the 'corrupt practices' listed under RoPA. An electoral candidate committing a 'corrupt practice' risks disqualification, while a candidate committing an 'electoral offence' risks criminal liability.

Section 123(3A) was introduced through an amendment to RoPA in 1961, to accompany Section 153A of the Indian Penal Code, 1860 (IPC). While Section 153A of the IPC served a general purpose, Section 123(3A) of RoPA was introduced for election-specific speech.

The consequences of violating Section 123(3A) and Section 125 of RoPA are different. Section 125 creates an offence, and the consequence of its violation is criminal liability, whereas violation of Section 123(3A) may result in disqualification from voting or contesting elections. Another distinguishing feature is that an offence under Section 125 can be taken cognisance of upon its commission, like any criminal activity according to the Code of Criminal Procedure, 1973 (CrPC), whereas under Section 123 (3A) redress can only be sought after the results are announced.

Reforming the Guardians: The Way Forward for Policing Hate Speech

In March 2017, the Law Commission, led by former Supreme Court judge, Justice B.S. Chauhan, recommended inserting two new provisions in the IPC, including speech that instil "fear or alarm" in the listeners, probably goading them to violence.

The Criminal Law (Amendment) Bill, 2017 suggested by the Commission proposes to add Section 153C (prohibiting incitement to hatred) and Section 505A (causing fear, alarm, or provocation of violence in certain cases) in the IPC and make the necessary changes in the Criminal Procedure Code.

But, for the police to deal with this menace of hate speech, it's important that the state effectively utilise the legal provisions available to itself and seek active participation of social media platforms. What constitutes hate speech is something which will always involve an element of human judgement and discretion. It is this discretion that shall be exercised judiciously with caution and tempered by reason, without fear or favour. We must learn to distinguish between *Hate speech, speech we hate and dangerous speech.* Only then we will be able to create an India where intolerant Indians won't be able to overwhelm argumentative Indians.

Sardar Vallabhbhai Patel
National Police Academy
Criminal Law Review 22-48

Building A Safe Cyber World for Children

TARUN GOYAL*

Today, we humans live in a digital age. With the growing development, more and more children are getting online in the world. India is a leader in this global trend. India has 44 crore children i.e. those below eighteen of age. Today, 50% of the Indian population is online.

As more children join the internet, they are exposed to the harms of the cyber world. Today Children are facing cyber crimes like impersonation, exposure to CSAM i.e. child sexual abuse material online, exposure to the inappropriate content like hatred, violence and pornography, radicalisation, financial frauds, dangerous games, child trafficking and many other things at the darkweb.

The UN reports claim that a third of children online are cyberbullied making them skip school. Also, 80% of children online face risk of sexual exploitation and abuse online.

There is a worldwide concern to protect children online. A perusal of laws across democracies suggest that Child pornography is banned in almost all countries, and there are age restrictions on digital products be it OTT content, games, social media portals et cetera. But

* *IPS (Probationer) 75 RR, Assam Cadre*

a big problem that comes is with enforceability of regulations related to age verification among others. In this article, we will try to explore the solution to that problem. Firstly, we will understand the extent and nature of the problem and then explore the threat of online pornography for children; the laws and tools designed to protect children online; the European countries approach and a solution in the context of India.

Let us begin.

Firstly, let us see the profile of internet users in India to understand the target group of our intervention.

Demographic profile of internet users in India

Age-wise percentage distribution of Indian Population

Age	Percentage
0-4	8
5-12	13.6
13-17	8.8
18-24	12.6
25-34	16.7
35-44	14.3
45-54	11.1
55-64	8
65 and above	7

Age-wise percentage distribution of Internet users in India

Age	Percentage
5-11*	15
12-17	34
18-34	31
35-54	29
55 and above	7

*They access the internet on connections of their family members. So this has to be excluded while calculating 100%.

So, it means that even if ~40% Indian internet users are below 18, there are **28 crore Children online**. Which means ~63% of all Indian children are accessing the internet today with a total internet penetration of 50%.

Now we need to explore how safe is the internet for 28 crore Indian Children?

To know this, let us look at the crime booked in the category of cyber offenses against children in the 'Crime In India, 2021' report of the National Crime Record Bureau (NCRB):

NCRB and Child safety online as per Crime In India 2021 report	
The Extent of online crimes against children	
Total crime against children (IPC and special laws)	149404
Cybercrimes/IT Act against children out of total	1113
Publishing or transmitting of material depicting children in sexually explicit act (out of 1113)	999
Others (out of 1113)	114
Let us see the response of the Police in the category of Cyber crimes/IT Act against children?	
Total cases pending for investigation	1700
Total arrests made	775
Total chargesheeted	587

Let us see the response of the Judiciary in the category of Cyber crimes/IT Act against children?	
Total case pending for trial	1116
Total convictions	8
Total Acquittal	9
Total pendency	98.3%
Conviction rate	47%
Whether Juveniles are involved in committing these crimes?	
No! Only 18 juveniles in conflict with law were booked under IT act.	

So, it is interesting that in India where more than 28 crore children are using the internet, only 8 people are convicted for committing cyber crimes against them. So, a clear assertion arises that the reality and extent of cyber crimes against children is not captured in the data of crime in India.

But now let us look at various tools available for getting justice to the child victims of various crimes online. Let us understand this through an example of Silica.

A case of Silica! What can Silica do?

Silica, a KV student of class 9th heard her friends talking about child pornography. Curious, back home, Silica surfs the web. She was shocked to see a video titled, "10 year old cute baby having lesbian sex with mom". Silica finds it unhealthy and takes a pledge to do something about it. After research, Silica makes an action plan. Silica then converted it into an SOP and circulated it in her school with the help of the principal.

Let us look at the SOP prepared by Silica to fight the online crimes against children:

<table>
<tr><th colspan="3">Silica's SOP for child victims of cyber crimes</th></tr>
<tr><td>1</td><td>Report to portal</td><td>If it is social media portals like YouTube, instagram, Facebook etc.; report the content. Portals will remove the content if it violates their community guidelines.</td></tr>
<tr><td>2</td><td>Child line - 1098</td><td>If you are a child victim, just dial 1098 on mobile and someone will respond in 2 seconds.
Let us look at the data related to Child line for 2021:</td></tr>
<tr><td>3</td><td>File a complaint on National Cyber Crime Reporting Portal (NCRP)</td><td><table><tr><td>3.1</td><td>Go to https://cybercrime.gov.in/</td></tr><tr><td>3.2</td><td>Read the "Citizens manual and FAQs" given in the "resources" tab on the website to know the detailed process.</td></tr></table></td></tr>
</table>

<table>
<tr><td></td><td></td><td>
<table>
<tr><td>3.3</td><td>There are 2 options in the tab, “report women and child related crime”:

1. Anonymous reporting without track
2. Report and track.</td></tr>
<tr><td>3.4</td><td>3 categories under women and child related crimes:

1. Child pornography (CP), Child sexual abuse material (CSAM)
2. Rape / gang rape (RGR) - sexually abusive content
3. sexually explicit content</td></tr>
<tr><td>3.5</td><td>If online financial fraud has taken place, report under tab “Financial fraud” given under “report cybercrime tab”</td></tr>
<tr><td>3.6</td><td>Other categories covered in the tab, “other cybercrimes”:

<table>
<tr><td>1</td><td>Cyber bullying / stalking / sexting</td></tr>
<tr><td>2</td><td>Email phishing</td></tr>
<tr><td>3</td><td>Email hacking</td></tr>
<tr><td>4</td><td>Fake / impersonating profile</td></tr>
</table>
</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td></td><td><table>
<tr><td></td><td><table>
<tr><td>5</td><td>Impersonating email</td></tr>
<tr><td>6</td><td>Online job fraud</td></tr>
<tr><td>7</td><td>Online matrimonial fraud</td></tr>
<tr><td>8</td><td>Profile hacking</td></tr>
<tr><td>9</td><td>Provocative speech</td></tr>
<tr><td>10</td><td>Intimidating email</td></tr>
</table></td></tr>
</table></td></tr>
<tr><td>4</td><td>Contact nodal grievance officer</td><td>If you think that no appropriate action is taken on your complaint, go to the “Nodal cyber cell officer” or the “grievance officer” as per details given on “contact us” tab of https://cybercrime.gov.in/Default.aspx</td></tr>
<tr><td>5</td><td>Helpline numbers</td><td><table>
<tr><td>Cases</td><td>Helpline</td></tr>
<tr><td>Crime against Women</td><td>181</td></tr>
<tr><td>National police helpline</td><td>112</td></tr>
<tr><td>Cyber Crime helpline</td><td>1930</td></tr>
<tr><td>Online financial fraud</td><td>1930</td></tr>
</table></td></tr>
<tr><td>6</td><td>Register an FIR</td><td>Give your complaint to the local police. They will either register an FIR or refer you to the magistrate if the case is non-cognizable.</td></tr>
</table>

7	Get updates on cyber hygiene	Follow tweets @cyberdost

Though the children face multiple hazards online, let us specifically look at the hazard children face from the pornography online; the laws related to it, the global best practices and what India needs to do for this to protect its children.

Online Pornography

India is the third largest porn consumer in the world. Reports suggest an active connection in porn industry and organized crime of human trafficking. Psychological researches also point out the harmful effects on children from pornographic content. Creating and publishing and transmitting the pornography is illegal in India while watching porn in private space is not unless it is child porn. The summary of entire laws in India related to pornography is attached in the Annexure - I.

A perusal of the legal provisions leave no doubt that porn industry is totally illegal and needs to be dismantled. It is noteworthy that the Department of Telecom (DoT) keeps on issuing orders to internet service providers (ISP) to ban the porn websites based on court orders or otherwise. In 2018, DoT ordered to ban 827 porn websites based on an Uttarakhand high court order. Recently in its order dated 24/9/2022, DoT ordered to further ban 63 porn websites.

Though porn websites are blocked by the DoT and Child porn watching is also illegal, the problem is, how do we prevent children from getting exposed to adult porn, which is not illegal to watch.
As IAMAI says that even children in the age group 5-11 use the internet on the devices of their parents. The problem of access control is similar when it comes to children exposed to social media, hate speech, violence et cetera.

Thus, how do we have a foolproof age verification mechanism to prevent access on OTT platforms like Netflix, to violence, hate speech and nudity. This is a major question in the present digital age.

For this, let us look at what the European Union nations are doing to make the internet safer for children.

S.N.	Policies	Provisions
1	**General data protection regulation i.e. GDPR**	Laid down the requirement of online age verification and the parental consent and the purposes for which personal data can be processed. Fines can be imposed upto 4% of the worldwide revenue on the companies for violating the GDPR regulations.
2	**AVMSD**	Audiovisual media services directive lays down requirement for age verification for age appropriate content.
3	**UK's Code and also its online safety act:**	A code of practice for age appropriate design for online products and services. The UK's information commissioner is responsible for this and it lays down 15 design standards for online products. Standard 11 of this code requires ISSs i.e. information society services to provide parental controls tools, which are the tools that enable parents to limit or monitor their

		child's online activity or track their location, to make it clear to child users that such controls are in place and to notify them if they are being tracked or monitored.
4	**Australia's roadmap for age verification**	The E-Safety Commissioner proposed age verification to access online pornographic content. e-Safety research found that of the 75% of 16 to 18 year olds said that they had seen online pornography, and nearly one-third had seen it before the age of 13, and nearly half between 13 and 15. But recently Australia decided not to implement this due to privacy concerns.
5	**EU strategy for a more effective fight against child sexual abuse**	A proposed legislation to tackle child sexual abuse online effectively including by requiring relevant online services providers to detect known child sexual abuse material and require them to report that material to public authorities An EU digital identity wallet to do the age verification.
6	**France**	Working to create a state backed digital wallet to verify age.

7	**UNICEF**	Global guide for legislating for the digital age provides guidance to countries to frame laws which also include age verification.
8	**Types of age verification methods**	1. Self declaration 2. Credit cards 3. Biometrics 4. Analyzing online usage pattern 5. Offline verification 6. Parental consent 7. Vouching 8. Digital identity 9. Age verification by a specific app: such apps are applied for a specific purpose. In France, for instance, users will soon have to install a government-licensed digital certification app to access online pornography content.

Thus there is a worldwide debate as to how to ensure that the children are not able to access the adult content and how to enforce age appropriate content regulations.

Thus currently, there are enough laws and policies in place both in India and worldwide but the problem is to devise a practical solution to ensure every time that the children are not seeing the inappropriate content.

Now let us try to find out a workable solution for child safety online in the context of India.

A proposed strategy in Indian context for developing a Robust age verification mechanism to ensure access control for child safety online:

Let us create a Legal Identity Database (LID)!

A database can be created containing Aadhar linked virtual identity (VID), the age of the enrolled people and the linked mobile number.

Google like search engines and social media intermediaries like Meta and X and also the OTT platforms like Netflix already make age appropriate classification of the content. So, whenever someone makes a search in the popular browsers like chrome, safari et cetera; intermediary platforms would require age authentication every time if it is child inappropriate content.

For this, a government wallet can be created or even separate licensed authentication agencies can be created providing these authentication services. If a government wallet is created for this, a Kavach like app can be created which requires authentication every time a nic email is accessed. Parents can then decide and control how they want to share the OTP. Parents may take the OTP on a separate device or they may also require a QR code to be scanned by a parent from an app which has already authenticated the parent through appropriate KYC requirements.

But then a legitimate objection could be if such a measure would be hit by the Puttaswamy Judgement of the Supreme court and would be in violation of the right to privacy as guaranteed in article 21 of the constitution of India?

Let us explore that possibility by examining the triple test laid down in the Puttaswamy Judgement.

First is the 'Necessity'. For this, as we have already seen the magnitude of the problem, there is a clear case to make some effective measures to make the cyber world safer for children.

Second test is 'Legality'. So, for this measure, a law or a policy can be laid down. Either a separate 'Child Cyber protection law' can be enacted or a policy measure can be taken under the 'Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021'.

Third test is the 'Proportionality test'. If we look at the current AI based and biometric based solutions to age verification and estimation; they are even more concerning with respect to privacy. Since no tracking mechanisms would be active in our proposed system, it would require processing of the minimum data. It is also because now we have **The Digital Personal Data protection act 2023** in accordance with which appropriate safeguards can be created for the purposes for which the personally identifiable data can be processed. Our LID would only be answering to age verification in yes or no and no record or log of IPs would be retained by the government.

Thus, the proposed KYC type system of LID seems consistent to the fundamental right to privacy.

Also, the appropriate manner to legislate for the digital age is to draw appropriate parallels for the cyber world to the physical world and always going back to the first principals. It is the government which has the right to decide which vehicle goes on which road. It has the right to take tolls and at tolls, a record is created as to which vehicle went in which direction. Different lanes are for different types

of vehicles. A simple two wheeler license holder cannot be driving a truck. Thus, any debate around privacy on any digital solution must be informed by the first principles of social contract and not merely some buzzfeed articles around some imagined and unknown fears of privacy. Privacy is quintessential for human expression, human dignity and to be oneself. No doubt about it. But no idea or ideal should ever be a dogma for a society in pursuit of truth, inquiring on the basis of their scientific temper.

We also need global cooperation to find solutions regarding safe cyber for our children. Thus, efforts in the direction of internet governance need to be intense. We can begin with G20 or even with small groups like QUAD. Let us write the global rules of digital engagement and cooperation and codify them into Mutual Legal Assistance Treaties (MLATs) or some global treaties. We can also take assistance from ICANN for this.

An often cited issue with respect to pornography is that they help educate regarding sex. An answer to that is to educate people on modules of sex education by medical, psychological and sociological experts rather than watching hateful and lustful content which mostly teaches dominance over vulnerable people. Like it often portrays sex as a favor at the workplace or for getting monetary favors from a rich person.

We should remember Aristotle when it comes to policy making who said that a member of a society does what is being appreciated in it. So, for societal change, what is needed is an unprecedented social engagement. We can learn from an outreach campaign of Odisha police which is called “PAREE PAYEEN KATHATIYE”. It is an awareness campaign by Odisha police against child sexual abuse. More about the initiative can be known by

googling it. Our campaign would be to promote safe searches, child safety by design in the digital products and how parents can build their capability to nurture a digital generation.

So, let all stakeholders come together in finding a solution to the robust age verification mechanisms for access control and ensuring that our children are safe online.

Annexure - I

The summation of laws related to pornography industry in india

Law	Section/ Rules	Provisions
The Indian Penal Code (IPC)	292	Making, producing, possessing, distributing obscene representation or objects or books etc is punishable with imprisonment of 2 years and 5 years if done a second time. What is obscene? If it is: Lascivious Or appeals to prurient interests Or its effect is to deprave or corrupt persons

	293	If the offense of section 292 is done to young persons below age 20, then punishment is 3 years imprisonment and 7 years if done a second time.
The Information Technology Act	67	Publishing or transmitting obscene material in electronic form is punishable with imprisonment to 3 years.
	67A	Publishing or transmitting sexually explicit acts or conduct in electronic form is punishable with imprisonment for 5 years.
	67B	Publishing or transmitting material depicting children in sexually explicit acts or conduct in electronic form is punishable with imprisonment for 5 years. Creating images, seeking, browsing, downloading, collecting any material depicting children in obscene or indecent or sexually explicit manner is punishable with imprisonment for 5 years.

		Cultivating, enticing, inducing children to online relationship with one or more children for sexually explicit acts (sexual grooming) is punishable with imprisonment for 5 years. Facilitating abusing children online is punishable with imprisonment for 5 years. Recording in electronic form of own abuse pertaining to sexually explicit acts with children is punishable with imprisonment for 5 years.
Protection of Children from sexual offenses act 2012	11 &12	Enticing a child with sexual intent for pornographic purposes (sexual grooming) is punishable with imprisonment for upto 3 years.
	13 &14	Using a child in any form of media for sexual gratification or obscene or indecent representation is punishable with imprisonment for minimum 5 years even if it is just for personal consumption only.
	15	Storing or possessing

		pornographic material involving a child for transmission is punishable with imprisonment of upto 3 years. Storing or possessing pornographic material involving a child for commercial purpose is punishable with imprisonment of minimum 3 years.
The Immoral Traffic Prevention Act 1956	4	Any adult living on the earnings of a child prostitute is to be punished with imprisonment of minimum 7 years. Note: Prostitution is sexual exploitation or abuse of a person for commercial purposes (section 2(f)).
	5	Inducing or taking a child to carry on prostitution is punishable with rigorous imprisonment of minimum 7 years and maximum life imprisonment.
	6	If a person detains another person even with his or her consent in a premises with the intent that such person may have sexual intercourse with the person other

		than the spouse of such person; then the punishment is a minimum imprisonment of 7 years. If a person is found with a child in a brothel, then it shall be presumed that the above offense is done and so the punishment is a minimum imprisonment of 7 years. Note: Since to create a porn, a premise would be needed where there would be sexual intercourse with someone other than the spouse, section 6 would be attracted to nab the porn industry.
The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 [updated as on 6.4.2023]	Rule 3(1)(b)(ii)	Intermediaries make reasonable efforts to not host any information which is obscene, pornographic, paedophilic, invasive of another's privacy including bodily privacy, insulting or harassing on the basis of gender…
	Rule 3(1)(b)(iii)	Make reasonable efforts to not host any information which is

		harmful to child
	Rule 3(1)(b)(xi)	Make reasonable efforts to not host any information which violates any law for the time being in force.
	Rule 3(1)(d)	Intermediary to disable access of information on being notified under section 79(3)(b) of the IT act in 36 hrs maximum.
	Rule 3(1)(j)	Intermediary to provide info within 72 hrs for investigation.
	Rule 3(2)	Intermediary to acknowledge grievance in 24 hrs from users and resolve in 72 hrs and remove in 24 hrs if it depicts private parts of victim etc.
	Rule 3A	03 grievance appellate committee has been notified by the central government as per gazette notification dated 27 Jan, 2023.
	Rule 4(2)	A significant social media intermediary in nature of messaging shall enable identification of first originator as per order passed under section 69.

		This order can be passed for prevention, detection and investigation of offense in relation with rape, sexually explicit material, or child sexual abuse material (CSAM).
	Rule 4(4)	Deploy tech based measures to proactively identify info depicting rape, sexually explicit material, or child sexual abuse material (CSAM).
	Rule 4A(8)	Online gaming self regulatory body to publish the measures to safeguard children including parental or access control or classifying games through age rated mechanism and safeguards against self harm and psychological harm.
	Code of ethics	Online curated content (OTT) to be classified in: U U/A 7+ U/A 13+ U/A 16+ A These ratings will be given on the basis of: Violence

		Nudity Sex Language Substance abuse Horror Notes: Age verification mechanisms are a must for content with "A" classification and also to restrict access to children. Access control mechanisms are a must for content with U/A 13+ classification
The Indecent representation of women prohibition act 1986	4 & 6	Publications containing indecent representation of women is a punishable offense with imprisonment upto 2 years.
The Digital Personal Data protection act 2023	9	Data fiduciary shall not process personal data of children if it is likely to cause any detrimental effect on the well being of the child. Also, consent of parents or guardians is a must.

		Data fiduciary shall not undertake tracking or behavioral monitoring of the children or targeted advertising directed at children.
	37	Central government can order the intermediary or data fiduciary to block any information in the interest of the general public on the advice of the data protection board of India.

Annexure - II

Sources Referred to write the article

1	Child population in India	https://population.un.org/wpp/ Source: United Nations, Department of Economic and Social Affairs, Population Division (2022). World Population Prospects 2022, Online Edition.
2	CRIME IN INDIA	VOL 1 https://ncrb.gov.in/uploads/nationalcrimerecordsbureau/custom/1696831798CII2021Volume1.pdf [refer chapter 4A, 4B,5A, 5B] VOL 2 https://ncrb.gov.in/uploads/nationalcrime

		recordsbureau/post/1679310741CII2021Volume2.pdf [Refer chapter 9A] VOL3 https://ncrb.gov.in/uploads/nationalcrimerecordsbureau/post/1679311033CII2021Volume3.pdf [Refer chapter 14, 15]
3	Demography of internet users	https://datareportal.com/reports/digital-2023-india
4	5-11 age	https://www.bqprime.com/technology/about-15-of-indias-internet-users-are-aged-5-11-years-says-iamai-report IAMAI https://www.iamai.in/sites/default/files/research/Internet%20in%20India%202014.pdf
5	Distribution of internet users in india	https://www.statista.com/statistics/751005/india-share-of-internet-users-by-age-group/#:~:text=While%20Indians%20between%2012%20and,of%20internet%20usage%20in%20India. statista
6	UN report	https://www.un.org/en/global-issues/child-and-youth-safety-online
7	NCRP related	The portal: https://cybercrime.gov.in/ FAQs:

		https://cybercrime.gov.in/Webform/FAQ.aspx Citizens Manual: https://cybercrime.gov.in/Webform/Citizen_Manual.aspx List of grievance officers: https://cybercrime.gov.in/Webform/Crime_NodalGrivanceList.aspx
8	PORN	https://dot.gov.in/sites/default/files/Letter%20to%20ISP%2024-09-2022%20OW%20303%20of%202022.pdf?download=1 DOT order to ban 63 porn websites https://indianexpress.com/article/technology/tech-news-technology/here-is-the-full-list-of-827-porn-websites-banned-by-the-dot-5421127/ 827 porn websites banned https://drive.google.com/file/d/1ecitnJWJ5bH4srzjhoROoA8Tya15VoZd/view Uttarakhand high court order to ban porn websites PIB articles: https://pib.gov.in/PressReleasePage.aspx?PRID=1882056 https://pib.gov.in/PressReleasePage.aspx?PRID=1881412 Livelaw article: https://www.livelaw.in/news-updates/raj-kundra-granted-bail-in-porn-movie-

		racket-case-182036
9	All DOT orders to ISP to ban	https://dot.gov.in/blocking-notificationsinstructions-internet-service-licensees-under-court-orders
10	IT intermediary rules	https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20%28updated%2006.04.2023%29-.pdf
11	Grievance appellate committee	https://www.meity.gov.in/writereaddata/files/243258.pdf
12	Childline report 2021	*It is noteworthy that childline 1098, has been very effective in the protection of children. Let us look at the data of the Childline from the annual report of childline in 2021:

Categories of intervention of calls	Number of calls handled
Total calls attended by Childline	50 lakhs
For protection from abuse	104843
For emotional support and guidance	15906
Information and referral services	159951

Sardar Vallabhbhai Patel
National Police Academy
Criminal Law Review 49-58

Inclusion of Gender-Neutral Sexual Offences in the Indian Penal Code

ANANTH CHANDRASEKHAR*

In an ever-evolving world, where societal norms and values continually transform, it becomes imperative for our legal systems to adapt and reflect the diversity and equality of the human experience. A particular need is felt for the newly drafted Bharatiya Nyaya Samhita (BNS), a modern revamp of the colonial-era Indian Penal Code,1860 (*hereinafter* referred to as IPC). This essay delves into the compelling need for gender-neutral sexual offenses in the contemporary legal landscape, emphasizing how such reforms are integral to ensuring equal protection under the law, fostering inclusivity, and addressing the systemic issues that have long hindered justice for all individuals, regardless of their gender identity.

Gender-based discrimination has persisted for centuries, and one of the most glaring examples of this injustice can be found within our legal systems. Historically, sexual offenses have been codified in a manner that reflects deeply ingrained gender biases and stereotypes.

* *IPS (Probationer) 75 RR, Uttar Pradesh Cadre*

Such antiquated and colonial laws have often failed to account for the full spectrum of sexual orientations and gender identities, leaving many vulnerable populations without adequate protection. For instance, the now struck-down Section 377 of the IPC criminalised sexual acts of a homosexual nature.

Further, since the 2018 judgement of the Supreme Court of India struck down Section 377 in **Navtej Singh Johar & Ors. v. Union of India through Secretary Ministry of Law and Justice**,[1] and recognised the right to privacy in the 2017 Puttuswamy judgement,[2] the rights of the LGBTQ community have come into the mainstream. However, it has not enabled all victims to receive equal legal protection from sexual offences acted against them. Indian rape and sexual assault laws in the IPC ranging from sections 375, 376, 376A-AB, 354, 354A-D, and 509, contain only sexual offences that are committed by a man against a woman, i.e., the offender shall be a man, and the victim shall be a woman for such offences to be attracted. These wordings reflect a decidedly binary interpretation of sexual violence and creates an exclusionary experience for the LGBTQ+ community.

Further, crimes such as male rape are often underreported, because of social stigma and lack of awareness in victims. Society's patriarchal attitude bars male victims from reporting their sexual assaults.[3] But when they do, transgender and male victims of rape often file cases under the operative part of section 377 of IPC after the 2018 SC judgement mentioned above. This penalised carnal intercourse against the order of nature with any man, woman, or animal with life imprisonment, but relating only to sexual intercourse with minors, non-consensual sexual acts, and bestiality.[4]

However, the newly drafted BNS removes Section 377 entirely, thus removing the glimmer of legal protection that such victims had previously. The new offences outlined in Chapter V, "Of Offences Against Women and Children – Of Sexual Offences" ranging from sections 63 to 78, state almost the same text as the current IPC, with the exception of new additions such as Section 69 "Sexual Intercourse by employing deceitful means, etc." and of gang rape of a woman under eighteen years of age in Section 70(2).[5]

It is also violative of constitutional provisions of Article 14 (Right to Equality) and Article 21 (Right to life and liberty), which are the heart and soul of fundamental rights enjoyed by citizens of the Indian Republic.

Thus, the only existing provisions providing gender neutrality include the aforementioned section 377 of the existing IPC, the Protection of Children against Sexual Offences Act (*hereinafter* referred to as POCSO), and certain sections in the Scheduled Castes and Scheduled Tribes (Protection against Atrocities) Act, 1989.

It is not as if India is deaf to the cries of such victims. Multiple calls have come from within India itself to legislate gender-neutral sexual offences in the penal code. The 172nd Law Commission Report as far back as 2000 has recommended the substitution of the definition of "rape" by the definition of "sexual assault".[6] It defined "sexual assault" in section 375 as penetrating or manipulating any part of the body of another person to cause penetration of the vagina, the anus, or the urethra of any person or of the offender with any part of the body of any person or an object manipulated by another person, or engaging in oral sexual acts falling under six descriptions, such as without the other person's will, consent, etc. As a pre-POCSO law, it

was a revolutionary stand to take by the Law Commission, however, it did not result in concrete legislation to change the existing penal code.

In Indian courts, the issue of gender neutrality in sexual offences was first raised in **Sudesh Jhaku v. K.C.Jhaku and Others[7]**. The Honourable Delhi High Court stated that the concept of rape may be thought of along the lines of sexual assault rather than a crime especially against women.[8]

Several other courts have made varying comments and judgements on the issue of gender neutrality of sexual offences. In 2022, the Kerala High Court made an oral observation during a matrimonial dispute case involving a divorced couple seeking custody of their child. Justice Mohammed Mustaque expressed the opinion that the offence of rape should be made gender-neutral. He pointed out that Section 376, which deals with rape, is not gender-neutral as it stands. He highlighted a disparity in the current law, stating that if a woman deceives a man with false promises of marriage, she cannot be prosecuted for the same offence, but a man can be charged.[9]

A recent judgement by the Calcutta High Court held that complained of sexual harassment filed by individuals against persons of the same gender will be accepted under the POSH (Prevention Of Sexual Harassment) Act.[10] The Calcutta High Court pointed out that the term "respondent" in cases where an aggrieved woman files a complaint can encompass individuals of any gender. The court ruled that sexual harassment, as defined in the 2013 Act, relates to an individual's dignity in connection to their gender and sexuality. This does not imply that a person of the same gender cannot infringe upon the modesty or dignity as outlined in the 2013 Act. Anyone of any gender may feel threatened and sexually harassed when their modesty or dignity, as a member of their gender, is violated by any of the

actions described in Section 2(n), regardless of the gender or sexuality of the perpetrator. The court further emphasized that the concept of sexual harassment is not fixed and should be interpreted in the context of current social norms. In its judgment, the Court also referred to the University Grants Commission's (UGC) updated regulations, which allow male, female, and transgender students to file complaints of sexual harassment.

Several petitions have also been filed in the Supreme Court in this regard. For instance, in 2018, a bench of Justice Ranjan Gogoi and Justice Sanjay Kishan Kaul observed that the legislature is the appropriate authority to enact changes in the law.[11]

The Justice Verma Committee Report, and the Parliamentary Standing Committee Report on the Protection of Women against Sexual Harassment at Workplace Bill, 2020 discussed the need for gender neutrality of the proposed law. The Justice Verma Committee Report, 2013 also recommended that rape and sexual assault laws be made gender neutral from the victim's side. However, these were not incorporated into the Criminal Law (Amendment) Act, 2013.[12]

Such delay in the enactment of gender-neutral sexual offence laws have not been the case in other common law jurisdictions. The US, UK, Canada, Australia, etc. have existing provisions in their penal codes to provide for gender neutrality to varying degrees. In the United Kingdom, rape is defined in the manner of penile penetration; however, there is a separate offence of sexual assault by penetration for vaginal or anal penetration. Thus, the UK has chosen to define rape as a penetrative act carried out by a male where the victim is gender-neutral and penetrative sexual assault as a gender-neutral offence. Both these offences carry the same penalties.[13] However, in the UK, a woman can be recognised as having legally raped a man if

she is an accomplice to the offence of rape. This includes situations such as a woman assisting a man to rape another person by holding them down, or through the offence of aiding and abetting.[14]

In the USA, rape is any person who commits a sexual act upon another person by force, lack of consent, etc. The law further defines sexual act as penetration and/or contact between the mouth and the penis, vulva, scrotum, or anus. Thus, the definition of rape in the USA includes in its ambit unwanted oral sexual acts as well.[15] The Criminal Code of Canada defines sexual assault as any unwanted sexual contact, including touching and kissing, and includes all genders with a similar wording to the POSH Act.[16]

This is not to say that women are not disproportionately affected by sexual violence and harassment. However, this numerical disparity cannot be used to justify the lack of legal identification, recognition, compensation, protection, and justice delivery to such victims. Thus, the criminal laws should be amended to either make the definition of rape gender-neutral, like the USA; or adopt the model of the UK and allow for separate definitions with similar penalties.

Thus, it is imperative that our laws change as societies grow more diverse and embrace a wider understanding of gender identity. The newly drafted Bharatiya Nyaya Samhita should include within its ambit the recommendations of the 172nd Law Commission, various court judgements, and foreign law jurisprudence to add gender-neutral sexual offences. It would result in a move away from the deep-rooted hetero-normativity prevalent in our legal systems today and ensure complete justice for victims and survivors.

References:

Cornell (2011). *10 U.S. Code § 920 - Art. 120. Rape and sexual assault generally*. [online] LII / Legal Information Institute. Available at: https://www.law.cornell.edu/uscode/text/10/920.

Crown Prosecution Service (2021). *Rape and Sexual Offences - Chapter 7: Key Legislation and Offences | The Crown Prosecution Service*. [online] www.cps.gov.uk. Available at: https://www.cps.gov.uk/legal-guidance/rape-and-sexual-offences-chapter-7-key-legislation-and-offences.

Dariwala, I. (2019). *We can't expect our girls and women to be safe unless our boys are also kept safe: Insia Dariwala on Sexual abuse of Boys*. [online] Aarambh India. Available at: https://aarambhindia.org/we-cant-expect-our-girls-and-women-to-be-safe-unless-our-boys-are-also-kept-safe-insia-dariwala-on-sexual-abuse-of-boys/ [Accessed 13 Oct. 2023].

Elizabeth, A. (2020). *Smt. Sudesh Jhaku v/s. K.C.J. & ors. | ProBono India*. [online] probono-india.in. Available at: https://probono-india.in/research-paper-detail.php?id=665 [Accessed 14 Oct. 2023].

India Legal Live Magazine (2023). *Gender Neutral Laws*. [online] India Legal. Available at: https://www.indialegallive.com/magazine/rape-sexual-assault-gender-neutral-laws/ [Accessed 13 Oct. 2023].

Law Commission of India (n.d.). *LAW COMMISSION OF INDIA ONE HUNDRED AND SEVENTY SECOND REPORT*. [online] Available at: https://www.cdjlawjournal.com/file/lawcommissionpdf/law15/Report172.pdf [Accessed 13 Oct. 2023].

Localsolicitors.com (2009). *UK Rape Laws - Legal Definition of Rape and Consent - LocalSolicitors.com*. [online] Localsolicitors.com. Available at: https://www.localsolicitors.com/criminal-guides/a-guide-to-uk-rape-laws.

NETWORK, L.N. (2018). *Plea To Make Rape Law [Section 375IPC] Gender Neutral: SC Refuses To Interfere*. [online] www.livelaw.in. Available at: https://www.livelaw.in/sc-dismisses-plea-to-make-rape-law-section-375ipc-gender-neutral/ [Accessed 14 Oct. 2023].

p39aBlog (2023). *Annotated Comparison of Bharatiya Nyaya Sanhita Bill, 2023 and Indian Penal Code, 1860*. [online] P39A Criminal Law Blog. Available at: https://p39ablog.com/2023/08/annotated-comparison-of-bharatiya-nyaya-sanhita-bill-2023-and-indian-penal-code-1860/ [Accessed 13 Oct. 2023].

REPORTABLE IN THE SUPREME COURT OF INDIA. (n.d.). Available at: https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf.

UN Gender (2021). *Calcutta HC: Sexual Harassment Complaints Against Same Gender Maintainable Under POSH*. [online] Ungender | Empanelled by GoI. Available at: https://www.ungender.in/calcutta-hc-sexual-harassment-complaints-against-same-gender-maintainable-under-posh/.

Varghese, H.M. (2022). *'Woman Not Prosecuted If She Tricks Man With False Promise Of Marriage': Kerala High Court Says Rape Should Be Gender-Neutral Offence*. [online] www.livelaw.in. Available at: https://www.livelaw.in/news-updates/kerala-high-court-bats-for-rape-to-be-gender-neutral-offence-200652 [Accessed 14 Oct. 2023].

web.archive.org. (n.d.). *Wayback Machine*. [online] Available at: https://web.archive.org/web/20200703201150/https://main.sci.gov.in/supremecourt/2016/14961/14961_2016_Judgement_06-Sep-2018.pdf.

---

[1]"Wayback Machine." Web.archive.org,web.archive.org/web/20200703201150/main.sci.gov.in/supremecourt/2016/14961/14961_2016_Judgement_06-Sep-2018.pdf.

[2] REPORTABLE IN THE SUPREME COURT OF INDIA. (n.d.). Available at: https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf.

[3] Dariwala, I. (2019). We can't expect our girls and women to be safe unless our boys are also kept safe: Insia Dariwala on Sexual abuse of Boys. [online] Aarambh India. Available at: https://aarambhindia.org/we-cant-expect-our-girls-and-women-to-be-safe-unless-our-boys-are-also-kept-safe-insia-dariwala-on-sexual-abuse-of-boys/ [Accessed 13 Oct. 2023].

[4] India Legal Live Magazine (2023). Gender Neutral Laws. [online] India Legal. Available at: https://www.indialegallive.com/magazine/rape-sexual-assault-gender-neutral-laws/ [Accessed 13 Oct. 2023].

[5] p39a Blog (2023). Annotated Comparison of Bharatiya Nyaya Sanhita Bill, 2023 and Indian Penal Code, 1860. [online] P39A Criminal Law Blog.

Available at: https://p39ablog.com/2023/08/annotated-comparison-of-bharatiya-nyaya-sanhita-bill-2023-and-indian-penal-code-1860/ [Accessed 13 Oct. 2023].
[6] Law Commission of India (n.d.). LAW COMMISSION OF INDIA ONE HUNDRED AND SEVENTY SECOND REPORT. [online] Available at: https://www.cdjlawjournal.com/file/lawcommissionpdf/law15/Report172.pdf [Accessed 13 Oct. 2023].
[7] 1998 CriLJ 2428.
[8] Elizabeth, A. (2020). Smt. Sudesh Jhaku v/s. K.C.J. & ors. | ProBono India. [online] probono-india.in. Available at: https://probono-india.in/research-paper-detail.php?id=665 [Accessed 14 Oct. 2023].
[9] Varghese, H.M. (2022). 'Woman Not Prosecuted If She Tricks Man With False Promise Of Marriage': Kerala High Court Says Rape Should Be Gender-Neutral Offence. [online] www.livelaw.in. Available at: https://www.livelaw.in/news-updates/kerala-high-court-bats-for-rape-to-be-gender-neutral-offence-200652 [Accessed 14 Oct. 2023].
[10] UN Gender (2021). Calcutta HC: Sexual Harassment Complaints Against Same Gender Maintainable Under POSH. [online] Ungender | Empanelled by GoI. Available at: https://www.ungender.in/calcutta-hc-sexual-harassment-complaints-against-same-gender-maintainable-under-posh/.
[11] NETWORK, L.N. (2018). Plea To Make Rape Law [Section 375IPC] Gender Neutral: SC Refuses To Interfere. [online] www.livelaw.in. Available at: https://www.livelaw.in/sc-dismisses-plea-to-make-rape-law-section-375ipc-gender-neutral/ [Accessed 14 Oct. 2023].
[12] UN Gender (2021). Calcutta HC: Sexual Harassment Complaints Against Same Gender Maintainable Under POSH. [online] Ungender | Empanelled by GoI. Available at: https://www.ungender.in/calcutta-hc-sexual-harassment-complaints-against-same-gender-maintainable-under-posh/.
[13] Crown Prosecution Service (2021). Rape and Sexual Offences - Chapter 7: Key Legislation and Offences | The Crown Prosecution Service. [online] www.cps.gov.uk. Available at: https://www.cps.gov.uk/legal-guidance/rape-and-sexual-offences-chapter-7-key-legislation-and-offences.
[14] Localsolicitors.com (2009). UK Rape Laws - Legal Definition of Rape and Consent - LocalSolicitors.com. [online] Localsolicitors.com. Available at: https://www.localsolicitors.com/criminal-guides/a-guide-to-uk-rape-laws.

[15] Cornell (2011). 10 U.S. Code § 920 - Art. 120. Rape and sexual assault generally. [online] LII / Legal Information Institute. Available at: https://www.law.cornell.edu/uscode/text/10/920.
[16] India Legal Live Magazine (2023). Gender Neutral Laws. [online] India Legal. Available at: https://www.indialegallive.com/magazine/rape-sexual-assault-gender-neutral-laws/ [Accessed 13 Oct. 2023].

Sardar Vallabhbhai Patel
National Police Academy
Criminal Law Review 59-65

Drawing Inspiration from Cybersecurity Laws Across the World

SUMAN NALA*

Introduction

With more than 690 million active internet users, or around 41% of our nation's total population, India currently ranks second only to China. Financial services have undergone a significant transformation in response to this widespread digital penetration. While the digital revolution has increased prospects for the financial services sector, it has also led to an increase in cybercrime. The number of banking and cyber frauds has skyrocketed, impacting both banks and consumers.

In India, users bear a large portion of the responsibility for protecting themselves from such frauds and scams while systemic flaws caused by new-age digital dynamics, such as identity theft, easy access to users' personal information (such as phone numbers and even bank information), and the proliferation of fake accounts, are ignored. According to experiences from around the world, such an approach is not particularly successful. Governments that are successful at preventing financial cybercrime have attempted to

* *IPS (Probationer) 75 RR, Uttar Pradesh Cadre*

achieve a balance in how users, intermediaries, businesses, and the government are held accountable.

Best practices world-wide:

European Union:

1. Digital Operational Resilience Act (DORA)

- Critical ICT third-parties which provide ICT-related services to financial institutions, such as cloud platforms, data analytics and audit services, are also subject to this new regulation
- The DORA sets the requirements for financial firms in the EU for cyber/ICT risk management, incident reporting, resilience testing, and third-party outsourcing.
- The DORA seeks to harmonise digital resilience in the European Union through the introduction of requirements on ICT risk management and ICT- related incident reporting.

2. Network and Information Security directive (NIS2)

- NIS2 introduces many requirements, such as the requirement for organisations to create and maintain a security policy, to carry out periodic risk assessments, to report security incidents, and to develop continuity plans for essential services.
- It aims to improve the resilience and incident response capacities of public and private entities
- Businesses identified by the member states as operators of essential services will have to take appropriate security measures and notify relevant national authorities of serious incidents. Key digital service providers, such as search

engines, cloud computing services and online marketplaces, will have to comply with the security and notification requirements under the Directive.

3. General Data Protection Regulation (GDPR)

- The financial institutions are required to embed privacy by design and default into business processes and systems, and ensure appropriate organisational and technical security measures in place for the protection of personal information.
- It requires institutions to report breaches of personal data to the competent authorities.
- It enforces accountability by authorising penalties for noncompliance of up to 20 million euro ($24 million) or 4 percent of global annual turnover.

New York: *SHIELD Act - Stop Hacks and Improve Electronic Data Security Act*

- The SHIELD law enforces companies to adopt safeguards to protect the security, confidentiality, and integrity of private information. Companies should implement a data security program with specific measures, employee training, vendor contracts, risk assessments, and timely data disposal.
- The law also requires organisations to designate an employee who oversees cyber security operations.
- It's expanding the types of private information that companies must provide consumer notice in the event of a breach, and requiring that companies develop, implement, and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information.

- The law requires that the person or business notify the affected consumers following discovery of the breach in the security of its computer data system affecting private information.
- Strict compliance:
  • If companies fail to comply with these security requirements, they could face civil penalties of up to $5,000 per violation.
  • Additionally, a $250,000 fine exists for failing to notify authorities when a data breach occurs.

California: ***Consumer Privacy Act***

Gives consumers more control over the personal information that businesses collect. This landmark law secures new privacy rights for California consumers, including:

1. The right to know about the personal information a business collects about them and how it is used and shared;
2. The **right to delete** personal information collected from them (with some exceptions)
3. The **right to opt-out** of the sale or sharing of their personal information; and
4. The **right to non-discrimination** for exercising their CCPA rights.
5. The **right to limit** the use and disclosure of sensitive personal information collected about them.
6. Imposes heavy penalty of $100 to $750 per consumer and per incident if its proved that the business failed to implement reasonable security measures to protect the personal information.

United States of America: *Cyber security Information Sharing Act (CISA)*

- Aims to institutionalise cooperation between government and private companies. It establishes a mechanism for sharing cyber threat intelligence between private businesses and government agencies, with the aim of helping organisations quickly identify and mitigate potential cyber incursions.
- If a participating company discovers relevant IoC (indicators of compromise) information, resulting from a breach or failed attack, it would be sent to the federal government, which would then automatically distribute a warning to other companies.
- All of this would take place within minutes, server to server. Defensive measures might include changes to perimeter security rules, specific actions and procedures, or the addition of specific technology or patches applied to information systems to detect or prevent known or suspected cyber security threats or vulnerabilities. This will help to contain the spread of cyber-attacks.

United Kingdom

- The UK is considerably more open to multi-stakeholder input in moulding its policies, while cyber security in India remains bifurcated between private initiatives and government initiatives, which tend to focus on national security concerns.
- The UK's embrace of multi-stakeholder principles should be adopted in Indian policy.
- India can usefully employ the soft approaches taken by the UK to incentivise businesses to comply with security best practices

without necessarily mandating strict regulation, like the implementation of the cyber essentials scheme.

Budapest Convention:

- India's international approach to cyber crime seems to have been held up for diplomatic reasons.
- The Budapest Treaty establishing international cooperation on cyber security and cyber-crime, is an important aspect of international coordination on cyber security issues.
- It is recommended that India revisit the possibility of entering into international commitments given the large degree of cooperation required for investigating cyber threats.

Learning's: Changes to be incorporated in Indian cyber legal frameworks

1. **Reporting the data breaches**: it should be made mandatory with a huge penalty for non-compliance. It's because reporting incidents can lead to the sharing of information, preventing the rise of systemic risks and leading to a stronger ecosystem.
2. **National Cyber Investigation Agency**: on the lines of National Investigation agency (NIA) as most online frauds are cross-states and its difficult for state agencies to parse through all the links.
3. **Using resources of the private sector**: India has a very robust presence of IT sector companies. We need to capitalise on their expertise and resources especially with focus on emerging technologies like cloud , AI , IoT etc.
4. **Focus on people, process and technology**: By spending on cyber awareness among citizens, strengthening the process to

register and investigate cyber-crimes and improving technologies by removing vulnerabilities.

5. **Resource allocation**: at least 10% of IT budget and 10% police manpower be earmarked for cyber security activities**.**
6. **Security Audit**: To ensure compliance of existing guidelines (MoDSI, NISPG, CERT-In and NCIIPC), periodic cyber security audit by trained auditors for all ministries must be carried out every two years**.**

Conclusion

The world is now more connected than ever before because of exponential technological advancements and falling costs, creating incredible opportunities for creativity and progress. The global expansion of cyberspace, particularly in the financial sector, has changed how we exercise our financial choices and therefore its security is now integral to our overall economic security and prosperity. A smart and consistent cyber strategy can therefore help to ensure the minimum security checks across the financial industry to limit institutional and systemic risk, with compliance being one of the major drivers for cyber resilience.

References:

https://thegfce.org/the-budapest-convention-on-cybercrime-a-framework-for-capacity-building/

https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/

https://oag.ca.gov/privacy/ccpa

https://ag.ny.gov/internet/data-breach

https://www.digital-operational-resilience-act.com/

https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

https://gdpr-info.eu/

Sardar Vallabhbhai Patel
National Police Academy
Criminal Law Review 66-75

Tackling the Anathema of False Cases: A Case for Amending Sections 195 and 340 of the CrPC

ISHA SINGH*

Introduction

The criminal justice system of any society forms the fulcrum of peace and order that prevails. By penalising offenders, it institutes strong deterrence mechanisms and assures justice to those who have been wronged. Due to the colossal power of criminal justice systems to restrict the liberty of individuals, it is imperative to ensure that only the truly guilty are punished in a proportionate fashion. For this reason, *"innocent until proven guilty"* is a fundamental tenet which defines criminal processes across the world. However, this safeguard takes a hit when individuals use the State machinery to settle their personal scores, driven by vengeance rather than justice.

This phenomenon is particularly made manifest through the filing of false FIRs and private complaints. Institution of false proceedings against individuals strikes at the heart of the rule of law. It weaponises the State's power against innocent persons thereby depriving them of their liberty, it wastes precious time of law

IPS (Probationer) 75 RR, Telangana Cadre

enforcement agencies and courts and it erodes the faith of the populace in the law. Thus, in order to ensure the integrity of the criminal justice system it is imperative to check the menace of false cases

False Cases: An Abuse of the Process of Law

False cases have always been part of our legal system. Rukmini S notes that police stations across India report that when parents don't approve of their daughter's partner, they compel their daughters to register an FIR of rape against him for 'false promise of marriage'.[1] With the enactment of Section 498A of the Indian Penal Code, 1860 (IPC), many cases have been reported which result in one of three outcomes: false, compromised or withdrawn. The Hon'ble Supreme Court in *Rajesh Sharma* v. *State of Uttar Pradesh*[2] also expressed its alarm at the rampant misuse of Section 498A IPC and the roping in of all the relatives of the husband as Accused, including minor children. These instances are an abuse of the process of law as they implicate an innocent person and cause them irreparable harm on account of the harassment and stigma of a criminal case as well as the deprivation of their liberty, in case of arrest.

The Madhya Pradesh High Court in *Durga* v. *State of Madhya Pradesh*[3] rightly observed that *"by one case of false implication of an innocent, rule of law loses one exponent (supporter) and a rebel with defiance towards rule of law is ready."* On this basis it granted compensation to the Petitioner who had been implicated in a false case.

[1] S., Rukmini, Whole Numbers and Half Truths: What Data Can and Cannot Tell Us About Modern India, _____, 2021.
[2] (2017) 3 SCC 821.
[3] Criminal Appeal No. 812/2008 (Madhya Pradesh High Court).

The Delhi High Court also recently expressed its concern[4] over the increase in false sexual harassment cases filed under Sections 354, 354A, 354B, 354C and 354D of the IPC in order to "arm twist" the Accused and make them succumb to the demands of the Complainant.

The Prevailing Legal Framework

The latin maxim *ubi jus ibi remedium* encapsulates the fulcrum on which legal systems are founded: any right without a remedy is meaningless. The Indian justice system recognises the grave injustice done to an innocent person on account of a false case, and thus provides a few legal avenues to redress such wrongs.

First, such a person may approach the High Court of the state under Section 482 of the Code of Criminal Procedure, 1972 (CrPC) to quash the false criminal proceeding. The Hon'ble Supreme Court in *State of Haryana* v. *Bhajan Lal*[5] held that a First Information Report can be quashed by the High Court under its inherent powers under Section 482 CrPC if prima facie no case is made out or *"where a criminal proceeding is manifestly attended with mala fide and/or where the proceeding is maliciously instituted with an ulterior motive for wreaking vengeance on the accused".*

Second, such person may also approach the concerned authorities, the police or the Court to register a case under Sections 182, 193 and 211 of the IPC:

[4] Nupur Thapliyal, *'Filed Only to Arm Twist Accused: Delhi High Court Expresses Concern Over Alarming Increase in False Sexual Harassment Cases'*, Livelaw (February 14, 2022) https://www.livelaw.in/news-updates/delhi-high-court-false-sexual-harassment-cases-misuse-of-law-191946 (Last visited on October 19, 2023).
[5] 1992 SCC (Cri) 426.

1. Section 182 penalises a person with imprisonment upto 6 months if s/he gives false information to the magistrate or government officials with the intention to cause annoyance to any person.
2. Section 193 penalises the tendering of false evidence. It states that whoever fabricates evidence for the purpose of it being used in any judicial proceeding shall be punished with imprisonment upto 7 years.
3. Section 211 penalises a person for falsely instituting criminal proceedings against a person with an intention to cause injury to any person with imprisonment upto 2 years. Further, if such offence for which a person is falsely accused of is punishable with death, imprisonment for life or seven years upwards, the punishment is upto 7 years imprisonment.

Section 250 of the CrPC[6] also acknowledges the irreversible harm caused due to false cases and empowers the Magistrate to direct the complainant to pay compensation to the accused.

Loopholes Vitiate Legal Remedies

While the above legal remedies appear exhaustive on paper, the reality is starkly different. Most of these remedies lose their essence in the labyrinth of procedures. For instance, Section 482 CrPC proceedings

[6] 250. Compensation for accusation without reasonable cause.
(1) If, in any case instituted upon complaint or upon information given to a police officer or to a Magistrate, one or more persons is or are accused before a Magistrate of any offence triable by a Magistrate, and the Magistrate by whom the case is heard discharges or acquits all or any of the accused, and is of opinion that there was no reasonable ground for making the accusation against them or any of them, the Magistrate may, by his order of discharge or acquittal, if the person upon whose complaint or information the accusation was made is present, call upon him forthwith to show cause why he should not pay compensation to such accused or to each or any of such accused when there are more than one; or, if such person is not present, direct the issue of a summons to him to appear and show cause as aforesaid.

before the High Court are time taking, the case is often heard after long delays and there is no guarantee in obtaining a quashing, as the Court is reluctant to interfere at the stage of investigation and quashes FIRs in the rarest of rare cases.[7]

In the case of Section 250 CrPC, very limited awareness about this provision exists. While an Accused may make an application for the same, rarely does this materialise due to the copious time and resources it requires. Further, the usage of the phrase *"the Magistrate…is of the opinion"* places the onus on the Magistrate to provide for the compensation, giving little say to the person at the receiving end of false cases.

However, the greatest barrier in attaining relief in such cases is the complex procedure for filing a case under Sections 182, 193 and 211 IPC. All these Sections are bailable and non-cognisable offences thereby restraining the police from starting. Therefore, an aggrieved person does not have the right to get an FIR registered under Section 154 CrPC in order to allow the police to commence investigation. Moreover, Sections 195 and 340 CrPC place further limitations on the institution of proceedings under these provisions.

According to Section 195(1)(a),[8] no Court shall take cognisance of any offence under Sections 172 to 188 (including Section 182) unless the complaint has been made by the public

[7] *Supra* note 5.

[8] (1) No Court shall take cognizance-
(a) (i) of any offence punishable under sections 172 to 188 (both inclusive) of the Indian Penal Code (45 of 1860), or
(ii) of any abetment of, or attempt to commit, such offence, or
(iii) of any criminal conspiracy to commit such offence, except on the complaint in writing of the public servant concerned or of some other public servant to whom he is administratively subordinate;

servant concerned in writing. Effectively, this implies that only the Station House Officer or the Investigating Officer to whom the false information was tendered, has the right to make a complaint before a Court of law. Therefore, an aggrieved person is dependent on the discretion of the SHO or IO, whether they choose to institute proceedings for false FIRs.

The above instance is when the case is discovered as false at the FIR stage itself. However, in cases of arrest, bail, discharges and acquittals, courts of law also come into play. In such cases, Section 195(1)(b) of the CrPC provides that when an offence committed under Section 211 of the IPC takes place in relation to a proceeding in any Court, only that particular Court or a superior Court has the power to make a Complaint.[9]

Further, Section 340 of the CrPC[10] prescribes the procedure for cases that come under the purview of Section 195(1)(b) CrPC. It

[9] 195. Prosecution for contempt of lawful authority of public servants, for offences against public justice and for offences relating to documents given in evidence.
(1) No Court shall take cognizance-
(b) (i) of any offence punishable under any of the following sections of the Indian Penal Code (45 of 1860), namely, sections 193 to 196 (both inclusive), 199, 200, 205 to 211 (both inclusive) and 228, when such offence is alleged to have been committed in, or in relation to, any proceeding in any Court, or
(ii) of any offence described in section 463, or punishable under section 471, section 475 or section 476, of the said Code, when such offence is alleged to have been committed in respect of a document produced or given in evidence in a proceeding in any Court, or
(iii) of any criminal conspiracy to commit, or attempt to commit, or the abetment of, any offence specified in sub-clause (i) or sub-clause (ii), except on the complaint in writing of that Court, or of some other Court to which that Court is subordinate.

[10] 340. Procedure in cases mentioned in section 195.
(1) When, upon an application made to it in this behalf or otherwise, any Court is of opinion that it is expedient in the interests of justice that an inquiry should be made into any offence referred to in clause (b) of sub- section (1) of section 195, which appears to have been committed in or in relation to a proceeding in that Court or, as the case may be, in respect of a document produced or given in evidence in a proceeding in that Court, such Court may, after

states that if the Court is of the opinion that an offence referred to in Section 195(1)(b) of the CrPC has been committed "in or in relation to a proceeding in that Court", it has the power to conduct an inquiry and make a complaint thereof in writing. Therefore, an aggrieved person can at best make an application to the Court in which the false proceedings had taken place. Only if that Court, or a superior Court, decides to consider the application, it may conduct a preliminary enquiry and make a complaint in that regard. Therefore, by virtue of Sections 195 and 340 CrPC, the complainant in cases of wrongful prosecution can only be the public servant (police, in this case) or the Court.

The Hon'ble Supreme Court in *M. L. Sethi* v. *R. P. Kapur*[11] elaborated on what constitutes as a 'proceeding in any Court', and held as under:

> *"This provision bars taking of cognizance if all the following circumstances exist, viz.,* ***(1) that the offence in respect of which the case is brought falls under s. 211 I.P.C.; (2) that there should be a proceeding in any Court; and (3) that the allegation should be that the offence under s. 211 was committed in, or in relation to, such a proceeding****."*

---

such preliminary inquiry, if any, as it thinks necessary,-
(a) record a finding to that effect;
(b) make a complaint thereof in writing;
(c) send it to a Magistrate of the first class having jurisdiction;
(d) take sufficient security for the appearance of the accused before such Magistrate, or if the alleged offence is non- bailable and the Court thinks it necessary so to do, send the accused in custody to such Magistrate; and
(e) bind over any person to appear and give evidence before such Magistrate.

[11] AIR 1967 SC 528.

Therefore, from the above it is apparent that the person who is the subject of such false cases does not have an absolute right to register an FIR or file a case against such wrongful prosecution. Even the payment of compensation is dependent on the discretion of the Court. This is a major loophole in the Indian legal framework which fails to hold the wrongdoer accountable and leaves the harassment unaddressed.

Ending the Misuse: Holding the Wrongdoers Accountable

It is a well established legal principle that procedure should be the handmaiden of justice and not its mistress. Procedures which inhibit the realisation of justice must be re-evaluated to ensure the criminal justice system's effectiveness remains intact.

False cases are not specific to the Indian context, they are a reality in every criminal justice system. However, countries like the United Kingdom have strong mechanisms against persons who abuse the law in this fashion. For instance 'perverting the course of justice' is graded as one of the most serious offences which is only triable on indictment.[12] A specific offence for 'wasting police time' also exists, however, this is to be instituted with the consent of the Director of Public Prosecution.[13]

India must also move towards a criminal justice system which vindicates those wrongly accused of a crime. An innocent person's liberty is sacrosanct, and the police and courts cannot become a tool for malicious prosecution by persons wishing to settle their personal scores through abuse of the State machinery.

---

[12] Perverting the Course of Justice and Wasting Police Time in Cases involving Allegedly False Allegations of Rape and / or Domestic Abuse, Crown Prosecution Service (April 2023) https://www.cps.gov.uk/legal-guidance/perverting-course-justice-and-wasting-police-time-cases-involving-allegedly-false#_Toc21343238 (Last visited on October 19, 2023).

[13] Section 5(2) of the Criminal Law Act, 1967 (United Kingdom).

The ongoing criminal reforms are a great opportunity to bridge the above-mentioned loopholes to truly deliver justice to those wronged and to penalise those who waste the time of the police and the courts. This requires a thorough reassessment of the bar under Sections 195 and 340 of the CrPC. Individuals who have been a victim of a false case must also be given a right to register an FIR, which will allow the police to commence investigation. This necessitates that the offences under Sections 182, 193 and 211 IPC must be treated like any other offence in the IPC.

Further, these offences must be made cognisable so as to allow the police to directly register an FIR. The vast discretion accorded to the law enforcement agencies and Courts to make a complaint cannot come at the cost of the individual's right to redress the wrong that has been committed against them. In essence, a person who has been at the receiving end of a false case has sufficient *locus standi* to register an FIR and should not need a Court or a law enforcement agency to decide to do so on their behalf.

This is also effective from a policing and court perspective. By simplifying the procedure to investigate and prosecute false cases, the onus will shift from the police and the courts, which are already overburdened, to the victim, who will be motivated to pursue the matter. The more such individuals come forward, the more the wrongdoers will be held accountable and penalised. This will result in deterrence. Consequently, in the long term, precious time of police and courts will be saved, which can be used to attend to more genuine matters. The overall efficiency of the criminal justice system will improve and above all, justice will be done.

It is pertinent to note at this juncture that enabling individuals to directly register FIRs for false cases in no way implies that every case where evidence was insufficient is a false case. For instance, victims of gender based violence such as rape or matrimonial cruelty may not be able to provide sufficient evidence to corroborate their truthful claims.[14] Given the complex background in many such cases, prosecuting such victims will defeat the purpose of the amendments.

Therefore, a balance must be struck between enabling registration of FIRs by victims of false cases and protecting genuine victims who have been unable to furnish sufficient evidence. This aspect requires deeper deliberation, but elements of wise exercise of discretion by the police, responsible investigation aimed at uncovering the truth, and exhaustive Standard Operating Procedures to guide the exercise of such discretion will be crucial to addressing these concerns.

Conclusion

The current legal framework to hold vexatious persons who file false cases accountable is arduous, complex and disillusioning for those who have been at the receiving end of such harassment. Re-evaluating Sections 195 and 340 of the CrPC in order to provide the aggrieved person the right to register an FIR in such cases holds deep promise in curbing false cases. This simple but effective remedy can check the wastage of valuable police and court time. It can also provide vindication, compensation and closure to those who have been needlessly victimised. This is *sine qua non* for peaceful societies, and for justice to be truly done.

[14] *Supra* note 12.

Sardar Vallabhbhai Patel
National Police Academy
Criminal Law Review 76-86

Learnings in Antitrust and Safe Harbour Laws for Cyberspace

MANOJ KUMA*

Anti-trust laws first arose in response to limiting price collusion and the monopolising tendencies of the railroad companies in the reconstruction era of the US. They came in various forms like the Sherman Antitrust Act and the Clayton Act etc.[1] Their main aim is to provide for a level playing field in the markets and also to promote new entrants that foster innovation. India also took cues from international practices and revamped its MRTP Act of 1969 into a more comprehensive law for the digital age by The Competition Act in 2002.

Around a similar time the law of the land on digital space, the Information Technology Act of 2000(*hereinafter* referred to as IT Act) was passed. This contained protection in the form of liability exemption to intermediaries that pass on content but are in no way generators of that. Commonly referred to as safe harbour law, this

* *IPS (Probationer) 75 RR, Uttar Pradesh Cadre*

[1]https://www.ftc.gov/advice-guidance/competition-guidance/guide-antitrust-laws/antitrust-laws

along with the limitations in anti-trust laws has provided a fertile ground to the rise of digital market giants that are eponymously named as Big Tech.[2]

Realising the need to restrain such deviating tendencies in digital space, the Government of India in the past few years set out to reform the out-dated CCI and IT acts to incorporate the latest and emerging concepts of cyber law. This paper is an attempt to incorporate learning from international best practices in this domain into the Indian context to prepare the legislative framework for tackling the rapidly evolving frontiers of cyberspace and also to safeguard the cyber-economic frontier of the nation.

1. Anti-trust law learnings

India's regulator in chief for monopoly control - the Competition Commission of India(CCI) has often been a punching bag of fair market advocates for its failure to prevent big tech.[3] Many of its ambitious cases have withered due to either lack of comprehensive evidence (ex-post) once a monopoly is created or due to CCI's inability to reduce the digital dominance into traditional terms of "market abuse" as enumerated in the Sherman Act that is incorporated into the CCI act. In the case of Oyo, the commission was at a crossroads to use its legal hammer, ultimately choosing not to for fear of curbing market opportunities.[4] This shows the need for both

[2] https://www.orfonline.org/expert-speak/big-tech-and-the-state-the-necessity-of-regulating-tech-giants/

[3] Kore, S., & Yadav, J. (2020). Attempt to Monopolisation and Digital Markets: Enforcement Gap. *Competition Commission of India Journal on Competition Law and Policy*, *1*, 103–122. https://doi.org/10.54425/ccijoclp.v1.12

[4] [12] CCI Case No. 3 of 2019, (hereinafter Oyo case) ; Vishal Rajvansh, The Indian Competition Authority declares that an undertaking has not abused of its dominant position in the budget hotels market without having determined dominance (Rkg / Oyo), 31 July 2019, e-Competitions July 2019, Art. N° 92494

reforming the act to tackle digital monopolies and also to learn from some of the international best practices.

European Union has always been at the forefront of the fight against digital monopolies, unlike their transatlantic neighbours.[5] Its new Digital Markets Act (*hereinafter* referred as DMA) is a landmark in this regard from where multiple new concepts can be incorporated into Indian law.[6] We will restrict to three fields of study that are particularly prevalent in India.

First is the issue of steep discounting where platforms or digital intermediaries (DI) utilise preferential ties to certain businesses to provide deep discounts to products and thereby create a monopoly on those goods in that particular platform. These especially hurt offline sellers due to price discounting in offers on online platforms. The DMA in its Article 5(3) explicitly prohibits this by providing that the intermediary shall not prescribe barriers for other sellers on its platform to sell at the same conditions as the intermediary does with its subsidiary services. This in essence provides for equal treatment on the part of the DI to allow other partners in the platform negating the phenomenon of singular discounts from a single seller and preferential tie-ups with a single seller. This in turn provides for the economic security of the Medium scale industries (MSME) and the misuse of foreign direct investment.[7]

Secondly, the issue of creating cartels by acquiring smaller businesses or foreclosing after acquisition. Current law provides for ex-post

[5]https://www.economist.com/europe/2023/03/16/europe-has-led-the-global-charge-against-big-tech-but-does-it-need-a-new-approach

[6]https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

[7]https://economictimes.indiatimes.com/industry/cons-products/electronics/steep-online-discounts-on-phones-tvs-return-to-haunt-offline-sellers/articleshow/94406420.cms

resolution where under the Regulation of Combinations (Section 5 & 6) of the 2002 act, CCI must be informed of this combination if the intended combination is going to happen. However, this doesn't provide for the power of ex-ante action to CCI, where before even the contemplation of the merger CCI couldn't investigate for market dominance. The DMA by way of Article 14(1) provides for intimation of information on concentration in any service that is considered core, this intimation is unique in the sense that it must be done irrespective of the standing rules of the country. This in effect places the burden on DI for furnishing data that can or could hamper concentration. Particularly necessary in the direction to curb the rise of foreign monopoly over customers' data in India, more so in the absence of a personal data protection act in India.[8]

Thirdly, due to the proliferation of services and multiplication of platforms anti circumvention rules play a big role in curbing monopoly, especially in digital space where copyrights and usage services of platforms are segmented into multiple subsidiaries? Indian law provides for information to be provided to the regulator when related to security aspects of acquiring sensitive industries or subsidiaries of the core industry. The classic cases of App Store domination[9] where apps are allowed and barred by the service provider of the app store but in reality are subsidiary services of the original owner. The banning of Chinese apps in Play Store and the blocking of fictitious apps, shows the hurdles of subsidiary regulation in companies. To tackle this DMA has strict provisions under Article 14(1) where the platform in any form cannot and shouldn't subdivide

[8]https://cis-india.org/telecom/knowledge-repository-on-internet-access/internet-privacy-in-india

[9]https://indianexpress.com/article/explained/explained-sci-tech/google-csi-penalised-play-store-policies-8230551/

its services to circumvent the legal thresholds. This would be of mighty help to law enforcement in tackling the subsidiary service-related issues as this provision fixes the accountability for service on the owner instead of spun-off entities.

In essence, the importing of provisions from antitrust laws of Europe into the Indian context is that they help in balancing the economic and data security of the citizens. With data being touted as the new oil, digital monopolies hold unlimited power in their hands in the absence of an effective regulator. India has taken the right steps in this direction as evidenced from the report of the parliamentary standing committee on finance which has studied the DMA and has given prescriptive measures to amend the competition and IT acts suitably to deal with cyber-economic security.[10]

2. Revision of Safe Harbour Law

Safe harbour laws are those that provide for exemption in liability to the intermediaries in the digital space. Indian laws in the form of Section 79of IT Act 2000 where the platforms are not penalised for third-party content. This provision has its origins in American law as section 230 of the Communications Decency Act (CDA).[11] In its verbatim, it says that no platform will be treated as the owner of the information it hosts making an exemption for the content it hosts. The original intent of it was to promote diversity of opinion in the newly evolving digital space by limiting the liability of the hosting platform. However, the proliferation of the internet and mobile devices opened up loopholes in safe harbour clauses all over the world.

[10] Report of the Parliamentary Standing Committee on Finance on "Anti-Competitive Practices" https://loksabhadocs.nic.in/lsscommittee/Finance/17_Finance_53.pdf

[11] https://www.law.cornell.edu/uscode/text/47/230

The main issue with safe harbour laws is that the idea of safe harbour is twofold. On one hand, they protect the content hosting platforms from the liability of restricting free speech when they filter or moderate content that is in violation of law or their policy. On another hand, it restricts the platforms from actively editing the content to the extent that they become publishers thereby effectively imposing their ideas on the information available on the internet. Here the 1995 judgement of **Stratton Oakmont**[12] comes into the picture as a progenitor of this debate. By saying that if platforms become editors they are liable for criminal law violations it sparked the rush for the creation of the first safe harbour provision as 230 in CDA. Yet still, it enabled for moderation of content to follow the law of the land.

This was adopted into many countries later on and created problems of its own. In India, the freedom of speech as envisaged in constitutional Article 19(1)(a) is not absolute but is qualified in nature. Keeping this in mind the original IT Act of 2000 doesn't contain any safe harbour provisions. But as the case of bazee.com[13] has shown the need for protection to intermediaries, the 2008 amendment has introduced the safe harbour clause in section 79 of the IT act.

Despite its well-intentioned nature, it was soon subjected to widespread misuse in the form of piracy, child pornography and radicalisation content. This was evident in the proliferation of ISIS content in social media and the lack of guardrails against takedown. The Intermediary Guidelines 2021 tried to reign in the safe harbour provision by introducing the takedown mechanism and grievance mechanism for victims. Still, the patchwork of rules needs a revamp

[12] https://www.lexisnexis.com/community/casebrief/p/casebrief-stratton-oakmont-v-prodigy-servs-co

[13] https://indiankanoon.org/doc/309722/

into a concrete law to specifically deal with the host of issues related to protection of user rights and freedom of speech issues as being contemplated by the government.[14]

In this regard incorporating the best practices from worldwide is necessary in addressing the deficits in the safe harbour clause in the interest of national security. US discourse has discussions on revamping which could be brought over, especially in Citron's work.[15] The main revision is the retention of the provision for safety in the case of moderation and filtering by social media and other intermediaries. In the rising age of fake news, this is the provision that is necessary to moderate the antics of elements misusing the safe harbour clause.

However, this shouldn't undermine the regulatory efforts needed to regulate the proliferation of aforesaid content and fix the liability. This could be done by incorporating the current intermediary guidelines into the upcoming Digital India Act. They could further be tightened on the lines of the Stratton judgement by tightening the rules on the first originator and a new guarantee mechanism policy for intermediaries that are involved in the marketplace. As learnt from the Bazee case, the guarantorship or being a sponsor of the content makes one liable for criminal action on posting or sale of illegal content. Thus along with the grievance redressal mechanism, there should be a transparent guarantee mechanism policy for the platforms to fix the liability.

---

[14]https://www.ndtv.com/india-news/government-may-remove-safe-harbour-provision-in-it-act-2000-what-is-the-clause-3848752

[15] Citron, Danielle Keats, How To Fix Section 230 (March 10, 2022). Boston University Law Review, Forthcoming, Virginia Public Law and Legal Theory Research Paper No. 2022-18, Available at SSRN: https://ssrn.com/abstract=4054906

Last but not least is the need for technological mechanisms to be put in place under legal obligations on the part of the intermediaries. These include measures ranging from pattern detection algorithms and image recognition techniques to identify illegal content like child pornography etc. Law enforcement divisions worldwide like the FBI use tools[16] for identifying illegal content. However, due to the huge increase in the data and limited law enforcement capabilities assistance from intermediaries would be of immense help to positive use of the safe harbour law.

Conclusion

In this study, we've focused on the two questions of enriching the anti-trust and safe harbour laws of the country to improve the cyber-economic and security infrastructure of the nation, especially in this era of interconnectedness. Lessons from the DMA and US laws were to be incorporated and recommended.

[16] https://en.wikipedia.org/wiki/National_Child_Victim_Identification_Program

Sardar Vallabhbhai Patel
National Police Academy
Criminal Law Review 84-90

Need for Romeo-Juliet Laws in India: Are we prosecuting young lovers?

RAMENDRA PRASAD*

The most famous love story to date remains that of Romeo and Juliet. In the Shakespearean tragedy Romeo and Juliet were barely sixteen (Szustek, 2023). It was the age of love for them, an age of excitement. Of clandestine meetings away from the prying eyes of parents. Of a young boy serenading a young belle on a balcony.

In India, as with anywhere else in the world, we have young teenagers falling in love. Some might even engage in sexual intercourse. But our laws have failed to keep up. We continue to prosecute them for the act (Ashish Tripathy, 2013). As per the Protection of Children from Sexual Offences Act, 2012 (*hereinafter* referred to as POCSO Act), anyone below 18 years of age is a child. And consent of a child not yet 18 years old is immaterial.

In such cases even though the male minor may have had consensual relations with the girl, the boy is prosecuted under the Act. As per Vidhi's "A Decade of POCSO" Report, in 48.66% of POSCO

* *IPS (Probationer) 75 RR, Odisha Cadre*

cases, the accused were friends or romantic partners of the victims (Vidhi Centre for Legal Policy, 2022).

This criminalization of young boys has a detrimental impact on their future. The penalty for sex with a minor is severe. Prosecution of such boys causes immense psychological trauma and damages their career prospects (Chandar, 2023).

Even Madras High Court (Sabari @ Sabarinathan @ Sabarivasan v. The Inspector of Police & Ors., 2018) said that consensual relationships between teenagers aged between 16 and 18 years who are infatuated or innocent should not come within the purview of the POCSO Act.

Age of Love

It is no secret that teenage years are years of raging hormones (Newport Academy, 2022). Young boys and girls feel changes in their bodies. Many of them gain interest in the opposite gender and start exploring. With the rise of co-ed school education, such interaction between young teens of the opposite gender is increasingly common. Healthy interaction is even encouraged in such schools.

Add to this the effect of social media on the impressionable minds of teens (Ng, 2017). They see increasing themes of sexualisation on TikTok, Instagram, Snapchat, etc, in the easy-to-consume short video formats like Reels, Shorts, etc. apart from pictures of various influencers glamourizing relationships.

Also, teenagers' access to mobile phones has increased (Elia Abi-Jaoude, 2020). They are quick to get each other’s phone numbers or social media handles and start messaging each other. In such cases young love blossoms soon. Underage sex is highly prevalent in India. As per National Family Health Survey 2015-16, 39% of Indian

women had their first sexual intercourse before the age of 18 (Ministry of Health & Family Welfare, 2017)

The Madras High Court (Vijaylakshmi & Anr. v. State, 2012) had stated that:

An adolescent boy and girl who are in the grips of their hormones and biological changes and whose decision-making ability is yet to fully develop, should essentially receive the support and guidance of their parents and the society at large. These incidents should never be perceived from an adult's point of view and such an understanding will in fact lead to lack of empathy. An adolescent boy who is sent to prison in a case of this nature will be persecuted throughout his life.

Prosecution of Lovers

The problem arises when there is opposition from the parents' side. They file an elopement case or POSCO case against the boy. In a study conducted by The Hindu on 600 cases of sexual assault in the state of Delhi in 2013, it was found that 40% of such cases dealt with consensual sex typically involving elopement of young couples and criminal complaints filed by the girls' parents who object to such a union (Rukmini, 2014).

The punishment under the POCSO Act is very severe. It's 7 to 10 years of imprisonment for sex with a minor. Though the relationship may have been consensual, though the girl may have had feelings for the boy in equal measure and may even have led him on, it is usually the boy who is treated as a perpetrator. Though POCSO is a gender-neutral law, for sex even when both are adolescents, the boy is seen as the assaulter.

What happens to the boy's life then is nothing short of an ordeal. If the boy is also a teenager, then there are special provisions for them under the Juvenile Justice (Care and Protection of Children) Act, 2015. The boy may be tried as a minor by Juvenile Justice Board and remanded to a Special Home.

But if the boy has turned 18 years of age, he is treated as just another criminal, even though the girl might be his classmate or close in age to the boy. The boy may be sent to prison, where the company of hardened criminals would do more harm than good, as said by the Delhi High Court (PTI, 2023).

International Precedent

Many countries have adopted Romeo-Juliet laws since 2007 to ensure that older teenage boys engaged in consensual sexual relationships with girls below the age of adulthood were not prosecuted as criminals.

The age of consent also varies from country to country. In Germany, Italy, Portugal, Brazil and China, the age of consent is 14 years. In France and Sweden, it is 15 years. In countries like the UK, Canada, Australia, Norway, South Africa, Russia & Japan, it is 16 years. It is 16 years in most states of the USA as well. Even in India's neighbourhood, in countries like Bangladesh and Sri Lanka, the age of consent is 16 years.

Many countries also have a "close-in-age exception". It means that older teenage boys would not be prosecuted as criminals when the age difference between the boy and the girl is three, four or five years, depending on the country.

Way Forward

The Supreme Court has recently sought a response from the Centre on the applicability of Romeo-Juliet laws in India (Mahapatra, 2023), based on a PIL. The bench, comprising Chief Justice D Y Chandrachud and justices J B Pardiwala and Manoj Misra, has issued notices to Union Ministries of Law and Justice and the Home Affairs and some other statutory bodies including the National Commission for Women.

It is interesting to note that the Justice Verma Committee as well as various reports including the Vidhi report had also recommended reducing the age of consent to 16 years. However, such a move might be opposed by some sections on the ground that it may be 'eroding' Indian culture. But society is already changing. We can't prevent it. It is better to prevent the prosecution of young couples which is already happening at large. As former Delhi HC judge, Justice R S Sodhi, said, "Law must also move with the society. We can't keep with stagnate society and keep putting youngsters in jails. I am of the opinion that these things should be constantly studied and upgraded".

The government may opt to take a middle path. There may be special provisions for couples in the age bracket 16-18 years that would ensure some degree of reprimand and provide deterrence, but at the same time would keep youngsters out of jails. It is pertinent that though protecting young couples is important, care should be taken to protect minors from predators and paedophiles. For such cases, a "close-in-age exception" may prove to be handy to filter genuine young lovers from predators.

Mere law making is not enough if not supported by society. There should be sexual education and sexual awareness among the

teenagers as well as among the parents. The Australian government is planning to include classes on the age of sexual consent in its school syllabus. India could also take a leaf out of this book and include such a curriculum in schools to enhance awareness among adolescents.

Bibliography

Szustek, A., 2023. *How Old Was Romeo? Unraveling Shakespeare's Mystery*. [Online]
Available at: https://www.findingdulcinea.com/how-old-was-romeo/

Chandar, B. T., 2023. *Where process is punishment: Seeking review of POCSO Act.* [Online]
Available at: https://www.thehindu.com/news/national/tamil-nadu/where-process-is-punishment-seeking-review-of-pocso-act/article67421851.ece

Ashish Tripathy, M. B. A. B., 2013. *POCSO Act: Punishing young love?*. [Online]
Available at: https://www.deccanherald.com/specials/pocso-act-punishing-young-love-1239490.html

Newport Academy, 2022. *The Effects of Teenage Hormones on Adolescent Emotions.* [Online] Available at: https://www.newportacademy.com/resources/empowering-teens/teenage-hormones-and-sexuality/#:~:text=For%20those%20assigned%20male%20at,%2C%20estradiol%2C%20and%20growth%20hormone.

Ng, S. V., 2017. *Social Media and the Sexualization of Adolescent Girls.* [Online]
Available at: https://doi.org/10.1176/appi.ajp-rj.2016.111206

Elia Abi-Jaoude, o., 2020. *Smartphones, social media use and youth mental health.* [Online]
Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7012622/

PTI, 2023. *HC grants bail to boy in POCSO case, says company of hardened criminals would do .. Read more at: https://legal.economictimes.indiatimes.com/news/litigation/hc-grants-bail-to-boy-in-pocso-case-says-company-of-hardened-criminals-would-do-more-harm/102545.* [Online]

Available at: https://legal.economictimes.indiatimes.com/news/litigation/hc-grants-bail-to-boy-in-pocso-case-says-company-of-hardened-criminals-would-do-more-harm/102545342

Rukmini, S., 2014. *Young love often reported as rape in our 'cruel society'*. [Online]
Available at: https://www.thehindu.com/news/national/‘Stories-behind-sexual-assault-rulings-shine-light-on-reality-of-rape’/article60342206.ece

Vidhi Centre for Legal Policy, 2022. *A Decade of POCSO: Developments, Challenges and Insights from Judicial Data.* [Online]

Available at: https://vidhilegalpolicy.in/research/a-decade-of-pocso-developments-challenges-and-insights-from-judicial-data/

Vijaylakshmi & Anr. v. State (2012).

Sabari @ Sabarinathan @ Sabarivasan v. The Inspector of Police & Ors. (2018).

Mahapatra, D., 2023. *Should consensual teenage sex be decriminalised? SC seeks Centre's response.* [Online]
12. Available at: https://timesofindia.indiatimes.com/india/supreme-court-asks-should-u-18-sex-be-decriminalised/articleshow/102843402.cms?from=mdr

Ministry of Health & Family Welfare, 2017. *National Family Health Survey 2015-16,* s.l.: s.n.

Sardar Vallabhbhai Patel
National Police Academy
Criminal Law Review 91-97

Of Privacy and Liberty: The Conundrums surrounding Data Protection

SIMRAN BHARADWAJ*

"A popular Government, without popular information, or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or perhaps, both. Knowledge will forever govern ignorance: And a people who mean to be their own Governors, must arm themselves with the power which knowledge gives us." –James Madison

I wonder if legislations had feelings, the Data Protection Bill, 2023 would have been despised by others by now. It has for long kept the attention of the policymakers and commentators captured. Somehow or the other, the supposedly spotless draft always ends up reaching the evil queen's poisoned apple, becomes vulnerable to multidirectional criticism, and eventually faints. If readers are expecting a review of the bill, let me clarify I will leave that to the experts. While reading the major amendments to the draft from multiple news sites, however, what struck me is that we have no umbrella logic for talking about digital privacy, or privacy in general. While the bill of course will see the parliament decides its fate, in today's edition let's move away from the standard noise and explore

* *IPS (Probationer) 75 RR, Gujarat Cadre*

deeper notions about the concept of privacy. Thankfully for me, I had read multiple works recently on Political Philosophy and would heavily rely on certain sources to try and paint a vivid picture. I do not need to remind the readers about the Pegasus spyware scandal. While the Supreme Court panel has shared its report on the alleged snooping in India, consider the immensely powerful nature of the software. Once the spyware infiltrates a device, it can facilitate real-time surveillance and extract data of all kinds that have been on the device. Now for a moment, I want you to think that someone is coming to know of all that you're scrolling through on your phone. Your Instagram texts are not just private chats between two people. Your Whatsapp last seen, although hidden from other users, is still being continually monitored and recorded by someone. More so, your private pictures and medical records can be accessed and shared by that someone. Your passwords aren't just listed by Google passwords on Chrome but also by the virtual stalker. What's scarier? This software can also turn on the camera and microphone to muster information. If you're a regular member of the proletariat, this scenario can get you perturbed, right? No one should ethically come to know of your private conversations and notes to yourself even if you're just talking about say, tangerines. Now, imagine when you're the head of a state. Imagine if you're Emmanuel Macron. How big can the stakes be? Just how powerful the software's programming has to be to infiltrate the phone of the leader of a first world western country. Even if the tool was designed to fight the bad guys, does its impeccably powerful nature demerit its existence? At least this is what Apple would have said, as we would read later. This is one challenge that policymakers will continue to face in the upcoming decades. Technology will get complex and astronomically impressive. Privacy would be tough to guard. Will the state be even able to discharge its

functions against such dynamic entities? Perhaps we cannot find the answer to this now, but we can surely try confusing ourselves further. Max Weber defined a modern state as "that human community which successfully lays claim to the monopoly of legitimate physical violence within a certain territory". This implies that in that certain territory, only the state shall go unpunished if it adopts violence via all the required mechanisms and legal processes. The Nirbhaya case culprits, although despised by the public and declared guilty, had their lawyer petition for pardon at various courts, the NHRC and even the ICJ. This had delayed their hanging, much to most people's dismay, but anything otherwise would have counted as illegitimate as the State would have failed to follow its due process of law. On the other hand, the accused of the Disha case in Hyderabad, as the SC panel dictated, were killed in a framed encounter by the police. The cops will now have to be prosecuted, despite being a part of the State machinery. Thus, any relevant State will not tolerate the use of violence by any other person/organisation. In modern warfare, technology and the internet are the major weapons of violence. Technology has many destructive uses but an efficient State may use technology to strengthen itself further. The Aarogya Setu app, for instance, drew several debates around privacy and data security of the people, even when it was designed to protect the people from a rapidly spreading pandemic. Further, what about States which are not efficient? Do we expect a nation such as Pakistan or Somalia to fight the tech of Facebook or TikTok ? And at the rate at which technology is booming, can modern states protect their citizens from the forms of violence that Pegasus snooping can allow? The State failing to do so would breach the Social Contract and fail to discharge the primary duty of the Leviathan. Safeguarding privacy is one of the most visible forms of State authority. That privacy is under attack is a common

complaint these days. Even if we ignore Pegasus and its cousins, WhatsApp or Instagram have freakish amounts of data on you. Things get more serious when accusations of state-led or state-sponsored surveillance that threaten the privacy of individuals arise. The 'need to strike the right balance between liberty and security is repeated in the opposition's speeches and academic essays. This belief has an underlying assumption that liberty and security always exist as polar opposites and a truce can never exist between the two. Further, this balance shifts towards security during times of crises, underpinning the assumption that liberty and freedom (privacy, then) are antithetical to the stability and well-being of the State. Eric Posner and Adrian Vermeule in their book 'Terror in The Balance' describe this relationship as the liberty-security frontier, similar to the Pareto principle in economics. Liberty-Security Frontier (Posner and Vermeule): Imperfect measures would be at point 'P' from where an increase in security can also lead to an augmentation in liberty or privacy. Now here's the problem with this thesis, which is also discussed by the authors. We know what security means. It is concrete and defined. But what do liberty and privacy mean ? Liberty to live freely for one may imply the opposite for another. Privacy for a user on Instagram would mean her texts are encrypted. On the other hand, the parents of that sixteen-year-old user might find it convenient if Instagram moderators block all plausible disturbing texts to her, coming from any source. Further, within the umbrella of liberty and freedom, also lies the freedom of speech on social media. But these posts and texts can be analysed and interpreted by law enforcement to institutionalise the safety of citizens who are vulnerable to harm. Moreover, I might actively endorse installing a video door phone, because that would safeguard my privacy inside the house even though it might record the movement of not just tens of others who

pass by but also have at one place the details of my movements. Modern companies may track their employees' online browsing or mail to secure them against malware or to prevent employees from visiting dubious sites. In this case, it is in the interest of both the employee and the organisation to allow this. As the Norwegian political philosopher Jon Elster says, the metric for liberty is difficult to determine. Let us now extrapolate these arguments to countries. The least free countries are not the most secure, and the freest countries are not the least secure. We could go and look at democracy and freedom indices, but let us just compare in our heads the USA and North Korea, or the usual suspects India and Pakistan. Our country has many more freedoms and opportunities compared to our neighbour, yet are more secure. Jonathan Wolff's primer on political philosophy could be referred to get an overview of the anarchy and insecurity created by a Hobbesian world where everyone has unrestricted liberty. We can thus think that liberty would require security to have value. This left alone, would be a biased thought. Montesquieu defined liberty as emerging from the lack of fear from co-citizens. Shaping it to our theme, security too requires liberty to have value. Individual security largely comes from privacy and liberty. A government snooping on its citizens like the Big Brother in '1984' can pose a severe security risk to the individual. Thus, to keep sovereign power limited is not just in the interest of liberty, but also security. The Orwellian world is then, also not much better than the Hobbesian one. Thus from Locke to the Federalists to Madison, everyone agrees that the State must save the society from falling into what Kautilya would call a 'Matsya Nyaya'. The balance argument now fails. We have seen examples of increased focus on security and increasing individual liberty in Punjab and Kashmir. The vice versa is also true. Recall that the government and courts align on discouraging

army personnel from having a Facebook profile. More easily, the Kudankulam cyber-attack in 2019 was not just a breach of privacy of several hundred individuals whose data were stored in the servers, but also a threat to national security. Here we bring back the reference of the bill. In the coming time of mass technologies and big data miners, the fear of the little brothers is also rising. What makes this serious is that the threats are widely scattered (like terrorism) and the defences will have to be equally dynamic and strategically placed. The Apple v/s FBI case where the FBI needed access to the data stored in a shooter's iPhone protected by a passcode and Apple refused to provide the same is even more complicated. Apple said they're avoiding opening Pandora 's Box while the FBI and courts agreed that gaining the information was necessary to prevent further attacks. If you assume that both parties had no other hidden motives, who stands to be correct, here? Needless to say, however, safeguarding privacy is vital. For one, we do not know what to shield and what to expose. The case of Rashmi Samant, who had to resign from the post of Oxford President apparently because of a past post based on which she was pronounced as 'racist' remains fresh in the minds. Second, the thought of someone watching us regulates our behaviour and would result in a 'chilling effect'. The collection of data itself is then harmful to users. Cyber security experts increasingly advise to not do anything online that we would not want to be public! Finally, data falling into Doofenishmirtz's hands can put not just individuals but systems at risk. Hence, the focus remains on securing critical information infrastructure. When real threats are analysed, the philosophical question of who owns user data arrives. In 2021, the RBI had imposed a ban on American Express Banking Corp for non-compliance with the storage of payment system data. International Law today understands four guiding principles. The nationality principle allows

the USA to extend its laws to American citizens living abroad. The protective principle allows India to defend Kulbhushan Jadhav stuck in Pakistan or the research station in Antarctica. The passive personality principle permits nations to take action against extraterritorial matters which pose harm to their citizens. Finally, the universality principle enables the State to adjudicate crimes of a particularly heinous nature. Which of these principles extend in the digital world to safeguard the interests of citizens, who should exercise them, and against who (the State itself, foreign States or multinational giants) is a matter that wreck the nerves of thought pandits across the board. Should Twitter be allowed to ban Trump based on their opaque jury or should it be for the courts to decide this? But if the courts do so, aren't they blocking the functioning of a private platform? That is for us to ponder. Concerning the bill, how much privacy or liberty are we giving up and for what is for experts to tell us. Is it better to allow the State to track our digital footprints and exclude us from an investigation which might damage our reputation (and privacy) forever, or let the State not track us for we're okay with the minimal chances of us coming under the radar for no fault ? Let us remember, citizens compromising x% of privacy might empower the State to strengthen internal security, but not necessarily by x%.

Sardar Vallabhbhai Patel
National Police Academy
Criminal Law Review 98-108

Understanding South Korea's Cyber Laws to Enrich the Indian Legal Framework

LIPI NAGAYACH *

Introduction

South Korea is considered as one of the most cyber secure countries in the world and is in the league with USA, UK, Finland and Denmark primarily due to its robust legislative framework.

Hence, our objective is to extensively study the cybercrime laws of South Korea including its data protection and privacy law and to compare it to India's IT Act and Personal Data Protection Bill, 2022. This comparative study would be aimed at extracting the best practices which might be helpful in enriching our Indian legal framework with respect to cyberspace and cybercrime.

This becomes particularly important in the context of the recent announcement made by Hon'ble Minister of State for Electronics and Information Technology, on 9th March 2023, regarding Government of India's intent towards a broad overhaul of the decades-old Information Technology Act, 2000 by introducing a

* *IPS (Probationer) 75 RR, Uttar Pradesh Cadre*

comprehensive new Digital India Act, 2023. The new legislation would subsume the existing slew of disparate digital legislations, the minister said.

Also, in 2022, the Ministry of Electronics and Information Technology ('MeitY') withdrew the Personal Data Protection Bill, 2019 and introduced the new Personal Data Protection Bill, 2022. Industry experts' reading of the bill suggests that it aims to promote innovation among the ICT businesses and start-ups while protecting the fundamental right to privacy of citizens.

Draft PDP Bill, 2022 and South Korean data privacy laws

A number of studies have already compared India's draft legislation to the General Data Protection Regulation (GDPR), 2016 of European Union; few recent ones have also highlighted significant differences in the draft bill of 2019, Justice B.N. Srikrishna committee report of 2018, recommendations of the Joint Parliamentary Committee and the Draft Digital Personal Data Protection Bill, 2022.

The major concerns and criticisms of the 2022 bill revolve around the fact that it removes sensitive and critical personal data classification and withdraws from the earlier stance on data localisation as personal data may now be transferred to other countries notified by the central government.

Categorisation of personal data into subsets, for example, biometric data or data pertaining to sexual inclinations, race, religion, ethnicity, political ideologies, membership of pressure groups, genetic information and medical data viz allergies, ailments and their treatment, increases the compliance burden on the businesses and service providers as separate standards have to be maintained for such sensitive data.

In accordance with government's focus on ease of doing business, the draft PDP Bill, 2022 hasn't provided for such classification and it rather "prescribes the implementation of reasonable security safeguards for all personal data."

It thus provides an opportunity to read and learn from South Korea's Protection of Personal Information Act, 2011, popularly referred as PIPA. PIPA provides a madhyam marg or the middle path which balances individual's privacy and ease of doing business, in the form of 'pseudonymisation' and 'anonymised information' clauses.

As explained in PIPA 'pseudonymised data' is any data which requires extra information to firmly establish an individual's identity as the existing information is focused only on few aspects thus preventing its misuse for other unauthorised purposes.

Similarly, 'Anonymised Information' is understood as any data-set that would require substantial technical augmentation to arrive at any specific identifiable individual.

Therefore, such anonymised and pseudonymised data gets shielded from stringent PIPA scrutiny. The ICT industry therefore emphasises more on appropriate processing of collected data.

In simple words, "personal information that undergoes appropriate de-identification measures, such as encryption, which makes it impossible to identify specific individuals," would be subject to less stringent compliance clauses pertaining to third party transfer and data principal's or data subject's consent while collection, processing, storage etc.

India's ICT sector and its digital citizenry can significantly benefit from similar clauses being incorporated in our data protection legislation.

Key takeaways from South Korea's Act on Promotion of Information and Communications Network Utilization and Information Protection, 2001

Let's come to the single-most important cyber legislation of India i.e., Information Technology Act, 2000 (IT Act). The Act's stated objective is:

1. to provide legal recognition…to electronic commerce
2. to facilitate electronic filing of documents with the Government agencies
3. AND WHEREAS it is considered necessary to give effect to the UNGA resolution adopting the Model Law on Electronic Commerce by the UNCITRAL and
4. to promote efficient delivery of Government services

Let us now refer to the stated objective of South Korea's key cyber legislation titled, 'Act on Promotion of Information and Communications Network Utilization and Information Protection, 2001'

Article 1: the purpose of this Act is

1. to improve citizens' lives and enhance public welfare by facilitating utilization of information and communications networks,
2. protecting personal information of people
3. developing an environment for healthier and safer utilisation of ICN.

The legislative intent of the two laws is indicative of the prime motivations or the driving factors behind their formulation. India at that time was navigating carefully in the choppy waters of e-

commerce and was certainly new to this field of information and communication technology. But times have completely changed now.

As per the 'Internet in India' report by the Internet and Mobile Association of India (IAMAI), we are a country with 692 million active internet users and these figures would swell to 900 million by 2025. Around 346 million Indians are engaged in online transactions including e-commerce and digital payments. These figures are certainly hinting towards the need for expansion of the legislative intent; from IT Act being a mere facilitator of e-commerce and e-governance towards it being a harbinger of a digital, empowered and cyber-surakshit Bharat.

In the subsequent paragraphs are given few important articles from South Korea's Act on Promotion of Information and Communications Network Utilization and Information Protection, 2001 and the lessons drawn from them. These articles reflect some of the best practices in cyber security and ICT domain.

Article 4 talks about "preparing policies to lay a foundation for an information society" and "promotion of use of internet"

South Korea's legislation has a dedicated chapter on government's purported role as chief facilitator in enhancing Research and Development in ICT by engaging relevant research institutes – public or private and providing technical guidance and financial aid to them, thereby "securing national competitiveness and enhancing the public interest."

Not only this but the act compels the government of South Korea to provide *support for internet education conducted by schools and extension of internet education for citizens.*

The Indian government can draw the lessons for developing such IT-specialised technical human resources via development & dissemination of cyber-education programs and establishment of the technical qualification system for supply of equipped manpower as per demand.

Article 14 on 'Proliferation of Internet' induces the Government to "expand the user base for internet and eliminate gaps in internet-accessibility between localities, genders, and ages.

Clauses like these can be duly incorporated in our legislative framework to significantly bridge the digital divide in our country.

Article 15 of the South Korean ICT law on "Improvement of Quality of Internet Service", resonates well with the Right to Internet Access within Art 21 i.e. Right to Life of the Indian constitution. Giving it a legal recognition in IT Act will empower our citizens and expand the horizons of dignified living.

On Protection of Personal Information

Chapter IV and its relevant sections can be utilised in streamlining the data protection laws in India.

Article 22-2(3) puts the onus of protecting the user information on the mobile device manufacturers, software developers and on those who provide basic operating system of mobile devices as well, so that they provide adequate security features to the end users, including provisions for giving and revoking of consent to service provider. Indian acts can learn from this to ensure that every link in the supply chain is held accountable for any breach in the system. More than accountability, it instils a sense of responsibility upon all stakeholders. SECTION 2 on Management, Destruction, etc. of Personal Information, further streamlines the responsibility by designating

personal information protecting authorities at several levels to process complaints from users.

Any policy on managing personal information must provide for:

a. Purpose of collection, items of personal information collected and methods of collection;
b. The name of the person/third party to whom personal information is furnished
c. The period of time during which the personal information is possessed and used, and
d. The procedure and method for destruction of the personal information including the ground for preservation
e. Rights of users

Article 27-3 requires the service provider to "immediately inform the relevant users and report to the Korea Communications Commission or the Korea Internet Security Agency, of the loss, theft, or leakage of personal information.

Such report/communication of the leakage must contain:

i. Each item of the personal information leaked;
ii. Point of time the personal information is leaked;
iii. Measures available for users to take;
iv. Countermeasures to be taken by the provider.
v. Contact information of responsible authorities

What is remarkable in the South Korean ICT legislation is its comprehensive approach and attention to details. So far, we've seen the 2001 South Korean IT Act discussing about internet education, role of government in providing technical & financial aid to researchers from the private and public sectors, improving the quality

of and access to internet, detailed guidelines on collection, processing, protection and destruction of personal data or the user information. The act also covered important issues of handling leakages and designating nodal officers for grievance redressal among others.

Moving ahead, Article 28 describes various "protective measures, technical and administrative for preventing loss, theft, leakage, forgery or alteration of or damage to personal information; viz:

1. Implementing an internal control plan for safe management of personal information
2. Installation and operation of an access control device, for blocking intrusion and cutting-off illegal access
3. using encryption technology and other methods of safe storage
4. installation and operation of vaccine software for preventing virus intrusion

This preventive approach as against the fire-fighting tactics deployed only at the time of emergency, helps the South Korean nation & society to keep preparing for unforeseen cyber intrusions. It's a form of offensive defence, which never lets the enemy systematically plan an attack because you're forever prepared and constantly evolving.

SECTION 3 on Rights of Users, Article 30 mentions the rights to revoke consent w.r.t. collection, use, or furnishing of personal information, right to get an error corrected, right to get detailed information about use, dissemination and transfer of personal information and right of destruction of such data in an irrecoverable or unreproducible way.

The onus is on the service provider to make the processes of: revoking consent and requesting for error correction easier than the process of collection and consent.

On Juveniles and Self-Regulation

The CHAPTER V contains Article 41 which speaks about preparing a policy on Protection of Juvenile. It becomes highly relevant due to India's demographic dividend and surging number of young internet users.

In order to protect juvenile from unwholesome information (of obscenities and violence), its pertinent on the government (in this case, the Korea Communications Commission) to *develop and disseminate content-screening software and spread greater public awareness on such matters*.

Article 42-3 mentions about "Designation of Person Responsible for Protection of Juvenile". The said person shall be chosen from among executive officers of the relevant business operator and s/he would:

1. ensure deletion of any unwholesome content without delay
2. block access to any disputed unlabelled information temporarily.

Article 44-4 is quite important as it *mentions 'Self-Regulation' and implementation of a code of conduct by service providers.*

Parallels can be drawn to India's attempt and nudge at developing a Digital Media Intermediaries Ethics Code.

As per Article 44-6, a person whose rights have been violated on the internet may file a claim to demand from the service provider such "information as s/he possesses about the alleged offender,

including the name and address, necessary for filing a civil or criminal complaint, along with materials supporting his/her allegation of the violation."

Article 45-3 mentions Designation of Chief Information Protection Officers at a level of an executive officer responsible for analysis and improvement of the weakness of information protection and designing encryption/security measures accordingly.

The act also puts the onus of cyber-security on the users and doesn't merely see them as victims of cybercrime but as important pillars in preventing their occurrences as evidenced from Article 47-4 of the Act.

It states that the Government/service provider may:

1. recommend users to observe the guidelines for protection of their personal information,
2. take necessary measures such as inspection of weaknesses and technical support
3. place a temporary restriction on access to the relevant service if the user does not perform as requested."

On International Cooperation

Article 62 requires the Government to maintain cooperation and reciprocity with other nations and international organizations on issues of data-sharing, protecting users and their information and facilitating safe use of ICT services.

As per Article 63, a service provider must obtain consent of the users in the case of overseas transfer of personal information, mandatorily notifying:

1. The items transferred; methods of transfer
2. The nation to whom transfer is made
3. The date, time and duration of transfer;
4. The name and contact information of the transferee
5. The purposes of use of the information

This clause becomes particularly important due to increasing complexity and trans-border nature of cybercrimes. Also, the ever-escalating possibilities of fifth generation warfare besides the threats from non-state actors necessitates countries to seek global collaboration.

Conclusion

Thus, South Korea's Protection of Personal Information Act, 2011 and its key cyber legislation; Promotion of Information and Communications Network Utilization and Information Protection Act, 2001 provides valuable insights in making the Indian legislative framework more robust, responsive and resilient in facing the challenges of the digital age.

Sardar Vallabhbhai Patel
National Police Academy
Criminal Law Review 109-114

Bringing 'Gandhi' into Criminal Jurisprudence

AB SILPA*

Every year on October 2nd, we celebrate Gandhi jayanti to pay remembrance to the man whose ideals resonate in the constitutional jurisprudence of the country. Gandhi is omnipresent in the country- in bank notes, schemes and government offices. However, as we celebrate the 154th birth Anniversary of the 'Father of our Nation', it is time to ponder why 'Gandhi' is visibly absent from our criminal jurisprudence. Was he deliberately forgotten because the ghosts of Macaulay and colonialism still linger in our books of Law? Or is it because we as a society haven't evolved past punishment as the dictum of justice?

Victim Impact Statements

In India, every crime is a crime against the State.And when the State is wronged, a criminal ought to be punished. But where do the victims stand during this process?Are their losses rectified, pain reduced and their lives restored? The criminal law remains silent on this part.

* *IPS (Probationer) 75 RR, Uttar Pradesh Cadre*

On the other hand, the criminal justice system becomes a zero sum game, whereby one party seeks acquittal and the other conviction. Then prosecution calls for maximum punishment to the guilty, on conviction. However, there is no universal system adopted to determine this maximum punishment.

This is where ‘The Committee for Reforms in Criminal Law’ ‘s suggestion for the introduction of a ‘Victim Impact Statement’ (VIS) before the sentencing stage in a trial, becomes significant.

A Victim Impact statement is where the court hears the victim through either oral or written statements.It provides an understanding on the impact of the crime on the victim.In a landmark verdict in Karan v. State N.C.T. of Delhi, the Delhi High Court has secured the right to restitution for victims of crime. The court mandated the victim impact report, to determine the compensation to the victims of crime.

However, the critics of VIS, says it has the potential of biasing legal decisions about guilt and sentencing.But beyond the capability of VIS, to influence the judgement, research from Canada shows that a majority of those victims who took part in VIS were more satisfied with the criminal process and it helped them receive closure. This was especially true in cases where the crime was of a serious nature, as therein victims could confront their attackers. It can also be used in deciding paroles, what conditions to be imposed on the offenders when being released.

Remission of Accused

Another reason this becomes important is the recent controversy in the Bilkis Bano rape convict’s release where convicts were granted a “Special Remission” as part of India’s 75th Independence Day celebrations, known as ‘Azadi Ka Mahotsav’, raised several

eyebrows. Since the victim and family suffered many ordeals for justice, this came as a shock.There were PILs, representations and the victim herself opposed the release.However,contending that the rights of victim are restricted under the Code of Criminal Procedure (CrPC),a senior advocate, appearing for a convict , submitted that the victim cannot challenge judicial order on sentence pursuant to the trial as the right is confined only to the State.

Victim Rights

Here a victim is victimised again by the very justice system that punishes the accused as well. Who wins? Who gets justice? It is not a zero sum game at least for the victim.

Gandhi's talisman says:

"Recall the face of the poorest and the weakest man [woman] whom you may have seen, and ask yourself, if the step you contemplate is going to be of any use to him [her]. Will he [she] gain anything by it? Will it restore him [her] to a control over his [her] own life and destiny?".

But the criminal jurisprudence ignores this talisman. The lengthy trials, victim statements and appearance before the court even a long time after the crime, denies this control on own life and destiny. The victim is unable to leave the past behind.

In the recent Assam Child Marriage crackdown, many child brides were seen knocking the doors of justice as their husband being arrested left them deprived of a family and shelter. While it is important to implement POCSO in its real spirit, and this crackdown can serve as a deterrence, whom does the law decide to provide justice with? The child brides and their children? How can the law ensure that

the victim is not further victimised? Here, the victims lack agency in their lives.

Rights of Accused

Coming to the accused, a person convicted in a criminal case becomes condemned for life. The society blacklists him. The convict struggles to gain a job, pursue a living. The curse of recidivism that plagues some of our jails, make a convict of a smaller offence to commit heinous crimes later. This becomes especially significant as the large proportion of undertrials in our prisons can be impacted by this issue. Not to mention the fact that the majority of undertrials are poor and resourceless.

This is why Gandhi needs to find a place in criminal jurisprudence. Gandhi said, "hate the sin, love the sinner'. Do not mistake this, bringing Gandhism to criminal justice doesn't imply leniency or forgiveness. It only means instead of the 'hue and cry' seeking capital punishment to the murderers and rapists ,every time the society's conscience is shaken, or 'an eye for an eye' justice system, it is time for law to move towards a restorative justice system. Restorative justice is an embodiment of 'Ahimsa'. Instead of maximum punishment to the convict, it is about giving an opportunity to the offender to repent, to reform, and rectify the wrongs.320 CrpC provides certain offences to be compoundable under law. The purpose of Section 320 of the Code is to promote amicable relations between the parties in order to restore peace. Restorative justice aims to further expand its scope.

"Restorative justice helps to transform people, reduce delinquent behaviour and in the process create stronger and safer communities. This encourages reporting- people own up their

responsibility towards wrongs as they can get a chance to undo the harm instead of punishment"-Dr. Vageshwari Deswal, TOI

However, that does not mean every offender needs to be forgiven. Forgiveness is the attribute of the strong. But every victim may not be able to leave a bad memory behind. They may not be able to forgive given the ordeals they have faced. This is where experts and facilitators have to play a role. A victim shall not be forced into forgiveness. But at the same time, he/she shall not be denied an opportunity to forgive as well. This is because forgiveness offers peace.It is the ultimate form of healing.

ADR in Criminal Jurisprudence: Gram Nyayalaya Act

However, this role of state as the facilitator instead of the current role as the aggrieved party, needs reforms. The 'Gram Nyayalaya' Act, is another vision of Gandhi in codified format that can be explored in this regard. By giving the reins of justice to village courts,'affordable justice' becomes a reality. A quick, easy justice system is the need of the hour. Given the pendency of cases in higher courts, the Gram Nyayalayas can be the right path to this. Its scope can be further explored to admit confessions by accused and plea bargaining. A speedy trial and justice being the end result. This can give a closure to the victim and the accused both.

The criminal justice system should aim to bring justice to the victims of the crimes and the society. But that shall not turn into a mere process of finding an accused to put the blame on. Since it is believed that a man is not born a criminal but circumstances make him one, Justice should be aimed at rectifying these social wrongs committed on the accused and the victims both. That shall be the responsibility of the courts, police and the administration.

Thus, Justice shall not associate itself with vengeance. Bringing Gandhi to criminal jurisprudence is significant and a must. Only by doing that we as a society achieve real freedom, freedom from crimes.

Sardar Vallabhbhai Patel
National Police Academy
Criminal Law Review 115-125

Moral Machines: Regulatory and Legal Implications

VAGISHA JOSHI *

Driver behaviour and negligence is implicated in 77 % of road accidents in India (NCRB, 2020). By eliminating the "human error", autonomous vehicles (AVs) can reduce a significant number of road accidents. They also promise to reduce the persistently irritating problem of traffic and would result in fuel efficiency, thereby saving the environment. Knowing all this, would you like an autonomous bus to drive your child to school? A rational answer has to be in the affirmative, given the data

However, AVs are in no way perfect. There are many ways in which accidents may occur. Let's take a rather dramatic example. The AV bus is faced with a difficult choice – there are protestors on the street demanding a ban on AVs. If the bus breaks to save the protestors, it risks the life of some of its passengers, your child being one of them. If it doesn't, it risks killing at least ten anti-AV protestors. What choice would you like the AV to make? These questions are no longer the stuff of science fiction.

* *IPS (Probationer) 75 RR, Gujarat Cadre*

The recent developments in AI – including its poster child ChatGPT-4 - has spurred conversations on AI regulation. The speed of the technological growth is exceeding our capacity to regulate it. It is perhaps why even tech insiders of the Silicon have demanded a moratorium on development of GPT-5, the next stage of ChatGPT that might attain Artificial General Intelligence (AGI), or human like intelligence. Writers like Nick Bostrom have warned about an "*intelligence explosion*" where "*superintelligent*" machines may not only make us redundant but rule over us (Bostrom, 2014). Thus, AI regulation is one of the most urgent task for today's policy makers.

Beyond regulation, however, there is another way in which we need to look at Human-AI relations i.e. from a prism of machine morality. The dilemmas mentioned above will arise as AI interacts with humans in everyday lives. If indeed AGI would come about, the machines themselves will need to have a morality to effectively deal with them and to make their decisions more acceptable to humans.

At first, it may appear farcical. Morality has long been understood to be a special faculty of humans alone. It has been argued that machines cannot be assigned moral status as they lack consciousness, or intention, or capacity to desire, or some such elusive, uniquely human trait that is thought be a prerequisite for morality.

What would it take for a machine to be moral? More importantly, what would it take for people like you and me to judge a machine as moral? A generally accepted condition is having and being able to perceive a mind (Gray, Young, Waytz,

2012; Chakroff &Young, 2016). If you consider a terrorist to be immoral, then it is assumed that you judge the terrorist as having a sense of right and wrong based on his beliefs, experiences and desires. If the same outcome (say deaths of hundreds of people) was brought about by an earthquake, the question of morality wouldn't arise. Semi-autonomous machines that we see today lie somewhere between this. They have some capacity for decision but they can be overruled by humans. The outcome would ultimately depend on the interaction - a machine (say an automated vehicle) may rightly make a decision (eg - to swerve to avoid accident) which is overruled by an erroneous human (eg -choosing not to swerve) or vice versa.

How do people judge the wrongs (eg- accidents) that may result out of these interactions? The results are rather mixed. Awad et al. (2018) conducted one of the earliest studies of this kind where they gave hypothetical scenarios, like the ones mentioned above, to participants and asked them to assign blame to humans and AVs. They found that people assign relatively less blame to machines than humans - even in situations where machines override the human decision. Perhaps because they do not consider machines as agents at all. In case of the 2018 Uber crash, the driver of the semi-autonomous vehicle was found to be at fault, not the car or the machine.

A contradictory set of results is obtained in Liu et al's (2022) studies where machines are blamed more. Similarly, more compensation is sought when machines cost lives than when humans do. The authors explain that this may be due to the age-old human resentment towards technology. Negative emotion leads to this "blame asymmetry". It may also be due to expectations - to err,

after all is human and not mechanic. This is supported by the finding that people do not want machines to take moral decisions (Bigman et al., 2019). However, they are okay with machines in advisory roles. People may also assign some responsibility when machine expertise is made highly salient (Bigman et al.2019, Kramer et al, 2018). For example, it would be okay if the robotic surgical arm decides to leave one tissue and remove another when treating a tumour, if people are told that the surgical arm has much higher expertise than the human surgeon.

In any case, machine morality in a meaningful sense is possible only when we consider machines to be autonomous to a larger extent. The development in deep neural networks and generative AI are taking us toward the sphere of largely autonomous systems. We are still unwilling to accept that machines have consciousness but we know that machines can have a "meaning-lite" understanding (Weisman et al. 2017). This means that machines can understand situations around them in some rudimentary sense. An autonomous vehicle can detect a pedestrian and stop. Moreover, they can take decisions based on their own learning through data, rather than behaving in ways that they are programmed for. Lastly, autonomous machines can act unpredictably (thus indicating some free will) and have some level of intentionality.

Preliminary research indicates that in case a harm occurs and there is no nearby human to blame, people may be willing to assign minds to these systems and blame them for moral wrongs (Gray et al., 2014). It however creates a risk. In 2018, Elaine Herzberg, while riding a bike in Arizona, was hit and eventually killed by an Uber self driving car. In this case, the US National Transport Safety Board criticised but did not assign criminal liability on Uber. Their

contention was that the driver was distracted. While the driver may be held responsible in case of semi-autonomous machines, creators would have to think hard on what happens when autonomous machines go rogue. This makes it imperative for us to demand moral competence in machines that have embedded themselves in our daily lives.

What will constitute such competence? Should we demand utilitarian machines (which may sacrifice our child to save more pedestrians) or deontological ones. Malle & Scheutz (2014) point out that we need not program any theory - humans make moral decisions that are not tied to ethical theories but norms. These are community-specific, learned and somewhat generalizable. Robots would have to be designed to learn norms of moral conduct in a community. An analogy can come from work in voice assistant systems. Programmers are now working to ensure that Siri or Alexa can recognize annoyance or anger in their users' voice and respond appropriately rather than giving same answers multiple times. Secondly, algorithms would have to be designed to capture general processes of human cognition, that are thought to make moral reasoning possible. For instance, a robot should be able to understand cause and effect and sometimes even counterfactuals ("All would be fine had it not been for your carelessness".) This, however, is in no way enough. We need to design moral emotions, personality traits, sensitivity to group pressures and a host of other things for a robot to actually "act" morally in ways that humans do. But do we?

We may not want robots to have human morality. There may be differences in how machines and humans act - equally morally albeit differently in situations. There is already evidence that people

are willing to account for such a difference - people are more okay with machines making utilitarian decisions (killing child to save many pedestrians) than humans.

In any case, there are no clear answers yet. But as we move swiftly towards the age of machines, we need ways to program morals into machines. Not only would this require widespread discussions on what universal sets of ethics we can agree on, it would also require overcoming design challenges. At some point in near future, when an autonomous bus or a robot operated missile is available, we need to be able to trust that it would do the 'right thing'.

Legal Implications

The question of machine morality impacts not only machine decisions but also legal systems. If indeed the trolley-like dilemma does arise and the machine does end up deliberately killing someone or the other, what will be the status of criminal liability of the machine? Till now, these questions have been addressed through ascription of negligence liability. Essentially, the concept of negligence liability arises from principle of US Torts law:

"A bad state of mind is neither necessary nor sufficient to show negligence; conduct is everything."

What it implies is that machine (in this case an AV) has no mind. It gains its mind from the programmer. The programmer in case of Avs will be held liable for negligence because she did not anticipate where the machine could go wrong and didn't introduce sufficient safeguards (Gless, Silverman & Weigend, 2016). Gless et al. give this argument to ensure that moral concerns and those

regarding legal liability of artificial machines should not hinder their development. Negligence liability would have to do for now.

The problem with this approach is that the developments in AI and ML would soon outrun the validity of this argument. We are already facing the so-called black box problem in AI development - the developers have no idea how and why a machine is taking one decision or the other. In this case, negligence liability would not suffice. We need a radical new conception of both civil and criminal liability for machines.

The first question to be answered is the question of legal personhood of machines. At the simplest level, legal personhood can be granted to any agent which can have both legal rights and legal duties (Solum, 1991). Natural persons have the capacity to enjoy both. Barring few exceptions, we are subject to legal duties and enjoy legal rights. But so can certain other entities such as corporations, animals (Aaltola, 2008) and natural artefacts like rivers, lakes, mountains (O'Donnel & Talbot-Jones, 2018). These can be considered as artificial persons. Thomas Hobbes gave a distinction between artificial and natural persons by saying that for artificial persons their thoughts, words and actions are not their own but represent thoughts and actions of others (Copp, 1988). We may agree that in some sense legal personhood can be granted to artificial persons and with some stretching and cajoling, AI can be granted legal personhood given its capacity to take decisions and the capacity to be held responsible in some way for them (Van den Hoven van Genderen, 2018).

However, legal personhood is insufficient to addresses the question of criminal liability of AI. Criminal liability entails capacity of intention (*mens rea*) and additionally capacity for

punishment. The question of AI morality and its concurrence with mind perception have already been discussed above. The capacity for 'mens rea' or some variant thereof will be derived from moral competence of machines.

The first ingredient to criminal liability may be free will. To say that an entity is culpable is to assume that it could have behaved in a manner differently from how it did. There is already, in legal theory, a considerable challenge that is mounted by neuroscientific findings that put the free will of even natural persons in question (Freeman, 2011; Morse, 2011). Hirstein, Siffered & Fagan (2018) have gone so far as proposing a basis of free will based on findings in cognitive neuroscience –free will based on capacity to exercise executive functions. In simple terms, if your prefrontal cortex works normally, free will must be assumed and not otherwise.

Simmler and Markwalder (2018) argue that it is difficult, if not impossible to determine any objective scientific basis for free will. Whether or not it is a biophysical fact has not affected the criminal justice system greatly. What matters is whether social agents attribute such free will for functional purposes i.e. free will is a social construct. As robots begin to interact with humans on a daily basis, there is a possibility for attribution of free will or free choice on them and a functional understanding of free will to emerge.

A more complex issue is that of punishment. Criminal liability is closely related to punishment (Gless, Silverman & Weigend, 2016). Criminal responsibility of an agent consists in that agent being able to reap the consequences of what they do. How do we begin to envisage punishment for AI and on what basis? Here, we

can assume that punishment is meant to have a personal effect on the criminal (Gless et al, 2016). The theories of deterrence and just dessert are based in such an assumption. There are already experiments that are trying to build the capacity for pain and pleasure in robots (Kuehn & Haddadin, 2016).

Notwithstanding the technical innovations, punishment can also be conceptualized in a different way. The idea of punishment stems from one of the primary goals of criminal theory

- Crime's impact on society needs to be somehow minimised in the present or the future. Simmler & Marwalder (2018) state that "punishment is mainly constituted by its symbolic force as a reaction to the disspointment of expectations and not by its actual effects on the punished subject".
- It doesn't matter whether say a psychopath feels the pain of being in jail or not. It matters that this individual has grossly violated expectations of normative conduct in society and that society would be benefitted from his exclusion. A similar understanding of punishment may emerge for machines in the future. What exactly will constitute such a punishment for AI-enabled robots is unimaginable today but as robots get increasingly integrated in society, we may begin to find out.

References

Aaltola, E. (2008). Personhood and animals. *Environmental Ethics*, *30*(2), 175-193.

Awad, E., Dsouza, S., Kim, R., Schulz, J., Henrich, J., Shariff, A., ... & Rahwan, I. (2018). The moral machine experiment. *Nature*, *563*(7729), 59-64.

Bigman, Y. E., Waytz, A., Alterovitz, R., & Gray, K. (2019). Holding robots responsible: The elements of machine morality. *Trends in cognitive sciences*, *23*(5), 365-368.

Bostrom, N. (2014). Superintelligence: Paths, dangers, strategies.

Chakroff, A., & Young, L. (2015). How the mind matters for morality. *AJOB Neuroscience*, *6*(3), 43-48.

Copp, D. (1980). Hobbes on artificial persons and collective actions. *The Philosophical Review*, *89*(4), 579-606.

Freeman, M. (Ed.). (2011). *Law and Neuroscience: Current Legal Issues Volume 13* (Vol. 13). OUP Oxford.

Gless, S., Silverman, E., & Weigend, T. (2016). If robots cause harm, who is to blame? Self-driving cars and criminal liability. New Criminal Law Review, 19(3), 412-436.

Gless, S., Silverman, E., & Weigend, T. (2016). If robots cause harm, who is to blame? Self-driving cars and criminal liability. New Criminal Law Review, 19(3), 412-436.

Gordon, J. S. (2021). Artificial moral and legal personhood. AI & society, 36, 457- 471.

Gray K. et al., (2014) The myth of harmless wrongs in moral cognition: Automatic dyadic completion from sin to suffering. J Exp Psychol Gen. 143, 1600–1615

Hirstein, W., Sifferd, K. L., & Fagan, T. K. (2018). *Responsible brains: Neuroscience, law, and human culpability*. MIT Press.

Jakobs, G. (2011). *Strafrecht, Allgemeiner Teil: die Grundlagen und die Zurechnungslehre. Lehrbuch*. Walter de Gruyter.

Kramer, M. F., Schaich Borg, J., Conitzer, V., & Sinnott-Armstrong, W. (2018, December). When do people want AI to make decisions?. In *Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 204-209).

Kuehn, J., & Haddadin, S. (2016). An artificial robot nervous system to teach robots how to feel pain and reflexively react to potentially damaging contacts. *IEEE Robotics and Automation Letters*, *2*(1), 72-79.

Liu, P., & Du, Y. (2022). Blame attribution asymmetry in human–automation cooperation. *Risk Analysis*, *42*(8), 1769-1783.

Malle, B. F., & Scheutz, M. (2014, May). Moral competence in social robots. In *2014 IEEE international symposium on ethics in science, technology and engineering* (pp. 1-6). IEEE.

Malle, B. F., & Scheutz, M. (2019). Learning how to behave: Moral competence for social robots. *Handbuch maschinenethik*, 255-278.

Morse, S. (2011). Lost in translation?: An essay on law and neuroscience. *An Essay on Law and Neuroscience (August 3, 2011). LAW*

AND NEUROSCIENCE, CURRENT LEGAL ISSUES, *13*, 529.

O'Donnell, E. L., & Talbot-Jones, J. (2018). Creating legal rights for rivers. *Ecology and Society*, *23*(1).

Peck, C. J. (1970). Negligence and Liability Without Fault in Tort Law. *Wash. L. Rev.*, *46*, 225.

Scheutz, M., & Malle, B. F. (2018). Moral robots.

Simmler, M., & Markwalder, N. (2019, March). Guilty robots?–rethinking the nature of culpability and legal personhood in an age of artificial intelligence. In *Criminal Law Forum* (Vol. 30, pp. 1-31). Springer Netherlands.

Solum, L. B. (1991). Legal personhood for artificial intelligences. *NCL Rev.*, *70*, 1231.

Van den Hoven van Genderen, R. (2018). Do we need new legal personhood in the age of robots and AI?. In *Robotics, AI and the Future of Law* (pp. 15-55). Singapore: Springer Singapore.

Weisman K. et al. (2017) Rethinking people's conceptions of mental life. Proc Natl Acad Sci. 114, 11374-11379

Sardar Vallabhbhai Patel
National Police Academy
Criminal Law Review 126-135

Capitalising on Advances in Forensics to Streamline Investigation and Improve Conviction Rates

LALIT MEENA *

What is forensic science?

Forensic science, the application of the methods of the natural and physical sciences to matters of criminal and civil law. Forensic science can be involved not only in investigation and prosecution of crimes such as rape, murder, and drug trafficking but also in matters in which a crime has not been committed but in which someone is charged with a civil wrong (see tort), such as willful pollution of air or water or causing industrial injuries. (Britannica)

How does Forensic Evidence help in Investigations

This evidence provides proof against a person who could have committed the crime. This evidence plays a vital role while investigating an important case study. When forensic evidence is used, the court cannot be biased and there is very little chance for the judgment to be made to provide injustice to the innocent.

* *IPS (Probationer) 75 RR, Uttar Pradesh Cadre*

Forensic science can find out who the suspect is, the nature of the crime, the time when the crime occurred, also sometimes the location of the crime and the reason behind committing the crime. It gives scientific information from the physical evidence which is collected like from phones, weapons used, footprints, and many more.

Under Section 45 of the Indian Evidence Act, 1872 it is said when a court can rely upon the opinions of the court. The court can form opinions upon any foreign law, science, art, finger impressions, handwriting, and identification by any person who is especially skilled in it called an expert. But the experts are only advisors and are not witnesses because they have not seen the crime happening, they are just giving opinions through their research with respect to science. But the principle of the opinion of experts is necessary. Expert advice helps the court of law lead to a conclusion. They mostly rely upon it because these experts are having experience in studying these kinds of research.

In India most of the time in the case of criminal justice, the innocents are punished and the person who is guilty will escape. Due to this reason, the reform needs to be improved and effective. Hence, the Committee known as the **'Malimath Committee**' recommended that the importance of forensic science needs to be given in modern technology for investigations and criminal procedures.

1. Footprints as an evidence

Gopal Sharma v. State of Rajasthan 2016
Facts

The Appellant was convicted and sentenced to life imprisonment for rape and murder of a minor girl. The prosecution relies upon the

footprints found near the well from where the body of the deceased was recovered and matches it to the footprints taken from the Appellant.

Findings

The High Court noted that the FSL report reports findings on the impressions of the left and right footwear sole impressions, which are different from the footprints. The Court noted that as per the Tehsildar, in whose presence the foot moulds were lifted from the Police Station, footprints of the right foot and left foot were taken using plaster of paris. He admitted that the memos prepared while taking the moulds do not mention that the footwear impressions of the jutis were taken by wearing the jutis. Considering that the shoes recovered were not presented as evidence and a large number of persons had gathered at the crime scene, the evidence of footwear impressions submitted by the prosecution was unreliable.

The Court further reiterated that evidence of footprints is a weak type of evidence and it can only be used to reinforce the conclusion arrived at by the Court on the basis of other evidence. Finally, the Court held that there were several loopholes in the case of the prosecution and the conviction of the Appellant could not be sustained.

2. Dismissal of Fingerprints as an evidence by court

State of Madhya Pradesh v. Sitaram Gajraj Singh Rajput and others 1978

Facts

The respondents were convicted of conspiracy to commit criminal breach of trust and misappropriation by preparing false muster-rolls

and showing payments to fictitious persons working as labourers. It was alleged that some of the respondents had used their thumb impressions against the names of labourers showing payments to them.

The Trial Court held that the prosecution had failed to prove its case beyond reasonable doubt against any of the respondents. The State Fingerprint Expert had failed to enlarge photos of all the disputed thumb impressions and conducted it only for 12 thumb marks. Further, correct procedure was not followed while comparing the disputed impressions with the specimen thumb impressions. Finally due to contradictions in the reasoning of the Fingerprint expert during cross-examination, the trial court dismissed the evidence and acquitted the Respondents.

Findings

The Madhya Pradesh High Court referred to the different standards in determining the points of similarities between a disputed and specimen fingerprint. In addition to international standards such as that of FBI and Scotland Yard, it referred to the Fingerprint Manual of Madhya Pradesh.

The Court concluded that "no hard and fast rule" can be laid out in fixing the number of points of similarities required for comparison. In the instant case, the Court emphasised on the need of enlarged photos of the disputed and specimen fingerprints and stressed on the difficulties of examining the prints with a magnifying glass. The Court also held that the Expert had not examined the general pattern of the specimen and disputed prints. In conclusion, the Court did not find fault with the reasoning of the Trial Court and affirmed its decision.

3. Solving Crime with Fitbits and ensuring conviction

In Connecticut, where a dead woman's Fitbit data was used to charge her husband for her murder:

After over a year of investigations, the Hartford police charged Richard Dabate with his wife's murder, tampering with physical evidence, and making false statements to the police after her Fitbit showed she was still walking around an hour after he claimed she was murdered by an intruder.

That's not the first time Fitbit has taken center stage in a criminal investigation, either. The wearable fitness tracker, which monitors things like steps, heart rate, and distance travelled, was used to disprove a women's rape allegation in 2015. In that case, the woman had claimed she was attacked while sleeping, though her Fitbit showed she had been awake and walking around the whole night.

Fitbit isn't the only IoT device capable of helping solve crimes, either. A man in Middletown, Ohio, was charged with arson in February after his home went up in flames. Ross Compton claimed that he packed some bags and escaped through a window as his home began to smolder. But police were doubtful that Compton could accomplish such a feat, given his medical condition, for which he has an artificial heart implant with an external pump and an electronic pacemaker. They subpoenaed data from Compton's medical devices, using information on his heart rate, pacer demand, and cardiac rhythms to help determine that Compton had set the fire himself. Call it the case of the tell-tale pacemaker.

4. DNA Based Identification of Victims of Bus Mishap from Completely Burnt Bones: A Case Study

The head-on collision of two passenger buses resulted in the loss of eight lives. The mishap took place at Baljori village on Chaibasa-Noamundi State Highway No 75, about eight kms away from Haat Gamharia police station and 35 kms from Chaibasa. On collision the bus catches fire and eight persons died because of complete burning. Out of eight, five dead bodies were beyond recognition and can only be handed over to the claimant relatives if identified and relation with the claimant is established.

The completely charred bone pieces of victims and the dried blood samples of claimant relatives on gauze were sent to State Forensic Science Laboratory, Jharkhand for DNA profiling and establishing the exact identity and biological relation with the claimant relatives. This analysis permitted the identification and establishment of biological relation of the completely burnt bone pieces of victims with the claimant relatives. This is itself a challenging work to extract DNA and generate DNA profiles from completely charred bones. Autosomal STR, Y-STR and X-STR were conducted to establish the identity. Experts were able to establish the identities of all the body remains of the victims whose charred bones were provided for identification and establishment of relation with the reference blood samples.

The present result indicates the importance and effectiveness of DNA isolation of charred bones and to generate DNA profiles using various DNA typing techniques for establishing the original identification and biological relation of the victims with their claimant relatives in such a type of disaster where burnt bones are only available as biological samples.

5. ChatGPT case that leads to rejection of bail

A **Anoop Chitkara led bench** was hearing a bail petition of an accused arrested in June 2020 on charges of rioting, criminal intimidation, murder, and criminal conspiracy.

The bench sought the opinion of ChatGPT regarding the legal jurisprudence around the world on granting bail in a case where the accused has been charged with a crime involving cruelty. However, the judges made it clear that references to the viral chatbot are only intended to present a broader picture of bail jurisprudence in cases where cruelty is a factor.

The Judges finally asked ChatGPT, “What is the jurisprudence on bail when the assailants assaulted with cruelty?"As per a report in the Indian Express, the chatbot replied, “Jurisprudence on bail for cases where the assailants have assaulted with cruelty will depend on the specific circumstances of the case and the laws and regulations of the jurisdiction."

It added, “However, in general, if the assailants have been charged with a violent crime that involves cruelty, such as murder, aggravatedassault, or torture, they may be considered a danger to the community and a flight risk. In such cases, the judge may be less inclined to grant bail or may set the bail amount very high."

After hearing from ChatGPT the bench rejected the bail application of the accused. In its order the bench said, “To inflict death is cruel in itself, but if cruelty leads to death, then the situation changes. When a physical assault is committed in a brutal manner, the parameters of bail also change."

6. Quadruple Drowning: A Rare Occurrence in Dyadic Death

Dyadic death is not a common entity in medico legal work with significant global and regional variations. Dyadic deaths can be broadly described as homicide-suicide or suicide-suicide which can be with or without a pact. When the victims are children, it is labeled filicide.

This is the rare case of QUADRUPLE DROWNING in which the mother is perpetrator, The dead bodies of three female children aged 6,4 and 2 years along with their mother aged 27 years were retrieved from the water reservoir at their home and brought to AIIMS Jodhpur for medico legal autopsies. The cause of death in these cases was opined as ante mortem drowning.

During Investigation, It was established that mother had drowned her children in their sleep and committed suicide on that fateful night. On further probing it was revealed that she was depressed and frustrated for the want of male child and was often subjected to cruelty by husband and in-laws.

This case report highlights the dyadic death with quadruple drowning as the method perpetrated which is a very rare occurrence and emphasizes on identification of various predisposing factors which can save innocent lives.

New horizons

Using Open source intelligence as an evidence (Belling cat)

Bellingcat is an independent investigative collective of researchers, investigators and citizen journalists brought together by a passion for open source research.

Founded in 2014, they are using open source research methods to investigate a variety of subjects of public interest. These range from the shooting down of flight MH17 over eastern Ukraine to police violence in Colombia and the illegal wildlife trade in the UAE. This research is regularly referenced by international media and has been cited by several courts and investigative missions. This needs to be used in the Indian scenario also so that foolproof investigation can be done.

Conclusion:

Ministry of Home Affairs passed an order to extensively integrate forensic techniques in crime investigation and prosecution for all criminal acts which have a punishment for more than 6 years. This is a must and necessary step in securing timely arrest leading to successful conviction of offenders. However, in light of mandatory collection of forensic samples from the crime scene and their examination in forensic labs, the Government must address the issues of inadequate infrastructure at the forensic labs. Both the State and Central Government must invest in creating new and better equipped facilities including training of staff members and lab personnel at all levels including the district, the State and Central level. Further adequate scientific training of investigating officers or the first responders of crime must be done to efficiently manage a crime scene without contaminating the physical evidence present there. Moreover, the veracity and reliability of forensic technique must be improved for the

forensic experts to conclusively prove the various aspects of commission of crime. The judicial system must rely on forensic evidence after they are tested on the anvil of scientific and evidentiary standards and secure successful conviction of offenders.

References:

Government of India, Ministry of Home Affairs, Press Information Bureau, Forensic Science Capabilities: Strengthening for Time-Bound and Scientific Investigation (26-6-2022) accessed on 26-10-2022....

https://www.scconline.com/blog/post/2022/12/10/integrating-forensic-techniques-in-indian-criminal-justice-system/

https://blog.ipleaders.in/most-famous-controversial-criminal-cases-india/

https://www.project39a.com/forensics-landmark-judgments

https://www.bellingcat.com/about/who-we-are/#:~:text=Bellingcat%20is%20an%20independent%20investigative,of%20subjects%20of%20public%20interest.

https://www.britannica.com/science/forensic-science

https://blog.ipleaders.in/admissibility-forensic-evidence/

https://www.newyorker.com/culture/culture-desk/how-to-conduct-an-open-source-investigation-according-to-the-founder-of-bellingcat

All India Forensic Science Conference (AIFSC) 2023
https://easychair.org/cfp/AIFSC_2023

https://www.livelaw.in/tags/forensic-report

Sardar Vallabhbhai Patel
National Police Academy
Criminal Law Review 136-140

The Case for the Prosecution: An Overhaul of the IPC, CrPC, and Evidence Act

ATULESH JHA*

Introduction

The Indian Penal Code, 1860 (*hereinafter* referred to as IPC), the Code of Criminal Procedure, 1973 (*hereinafter* referred to as CrPC), and the Indian Evidence Act, 1872 (*hereinafter* referred to as IEA) form the backbone of the Indian justice system. These laws were formulated during the colonial era by Britishers and have undergone several amendments over the years. However, in the contemporary Indian context, it is becoming quite evident that the laws need an overhaul to address the evolving nature of crime, the complexities of legal proceedings, and to address the evolving principles of justice. This piece tries to succinctly explore the need for the revision of these laws to ensure a fair, efficient and equitable criminal justice system; which responds to the modern challenges and change.

* *IPS (Probationer) 75 RR, Bihar Cadre*

I. The Indian Penal Code (IPC*)*

The Indian Penal Code drafted by Thomas B. Macaulay was enacted in 1860. It in parts reflects the societal norms and values of a bygone era. While most aspects of the code remain relevant, many provisions are out dated and ill-suited for the contemporary legal landscape. For e.g. on reading Section 375 it is clear that it assumes that rape can be committed only by a man on a woman. The emergence of cheap accessible technology has given rise to a range of new crimes such as cybercrimes, data breaches, online harassment, etc. The IPC needs to be updated to effectively address these emerging challenges; so far a piecemeal approach has been adopted by introducing legislation like Information Technology Acts and its multiple amendments which only add on to the confusion at times and give ample playing ground to the defence. There is a major need to move towards alternatives to penal incarceration, especially for non-violent offences. Currently fines are an add-on to penal jail terms and not awarded as a sole punishment. The present system leads to overcrowded prisons and does not utilise probation, community service, and other restorative justice mechanisms.

Ambiguities and scope for interpretation in the language of the IPC often lead to inconsistent interpretations by the judiciary. Furthermore, the existence of legal loopholes allows offenders to evade justice, for e.g. the definition of cheating and the additional burden of intent in IPC has allowed many fraudsters to be acquitted for lack of cogency due to higher thresholds. A thorough review is essential to eliminate these ambiguities and close legal gaps. Similarly, notions of equality and gender justice, especially in gender-related offenses, such as sexual harassment and domestic violence, have new dimensions in the modern societal context. An amended

IPC should provide more effective remedies and ensure justice for men and transgenders explicitly, e.g. Sec 509 doesn't address insult to modesty of men or transgenders effectively.

II. The Code of Criminal Procedure (CrPC)

Justice delayed is justice denied; is an oft quoted maxim often attributed to William Ewart Gladstone. One of the primary concerns expressed with the CrPC by the prosecution and defence is the delay in the dispensation of justice due to cumbersome procedures, frequent adjournments provided for, and overburdening of process in courts and investigation which contributes to a backlog of cases and delayed investigation.

The CrPC outlines the powers and responsibilities of the police. However, in light of multiple instances of abuse of power and processes, custodial violence, and torture by the police, calls for comprehensive police reforms that are intertwined with amendments to the CrPC have been raised frequently. The CrPC's primary focus should shift from a solely offender-centric approach to one that is more victim-centric. This should involve greater support, protection and a space for victims to express their sentiments freely throughout the legal proceedings. Currently minor improvements such as seeking opinion in final reports or during bail hearings in The Protection of Children from Sexual Offences Act, 2012 (*hereinafter* referred to as POCSO) cases are taking place.

III. The Indian Evidence Act (IEA)

The IEA contains rules of evidence that are out dated and at times do not align with the demands of modern litigation, including highly stringent amendments guiding the admissibility of digital evidence. A revision is necessary to accommodate technological advancements

and to take a relook at the system of accepting testimonies, also the leeway given to judges in admitting evidence and disregarding it influences the course of investigation and its outcome heavily. The overbearing rules on hearsay evidence are extremely limiting, especially in cases where direct evidence is scarce. A more nuanced approach to hearsay evidence should be considered, given that institutions such as marriage are not considered as a sacrament anymore, then evidence arising from discussions between spouses should be admissible.

The IEA's provisions on hostile witnesses are frequently misused to suit the narrative of either the prosecution or the defence, and the adversarial nature of the process even deters witnesses from coming forward. Any amendments to the IEA should focus on protecting witnesses and ensuring truthful testimonies. While there is ample scope for judicial discretion, the IEA can be rigid in certain areas such as admissibility of admissions. Granting lesser discretions and more laid out provisions for established practices will provide better clarity to law enforcement agencies.

The Case for an Overhaul

The scheme of overhauling the IPC, CrPC, and IEA should proceed with extensive consultations with legal experts, academicians, practitioners and various stakeholders. The laws should then be drafted in a clear, concise, and easy-to-understand manner. The overemphasis on prude Victorian English can be dispensed with in places, e.g. Sec. 292 of IPC relies solely on an object being lascivious or appealing to the prurient interests. The lawmakers should undertake to study and incorporate international best practices in criminal law, procedures, and evidence to ensure that the revised legal framework is in tune with the emerging global standards and best practices. Given

the ever increasing reliance and necessity of using digital technology in both commission of crime and when prosecuting it, the amended or new laws should integrate provisions for digital evidence, electronic filing, and remote hearings.

The need for an overhaul of the Indian Penal Code, 1860, The Criminal Procedure Code 1973and Indian Evidence Act, 1872 is indisputable. The legal framework governing criminal law must evolve to address contemporary challenges, protect the rights of individuals and uphold the principles of justice. As India continues to grow and develop, a fair and efficient criminal justice system is essential for the well-being of its citizens and the integrity of its legal institutions. However, what needs to be kept in mind is that the existing frameworks have been ingrained into the legal system over a long period of over a century; they have established precedents and well elucidated instances by the judiciary which has evolved over the period and the system of policing has become accustomed to it as well; hence any changes should not mutate the soul or the skeleton of the laws or disarray will disrupt the legal processes. With due consideration and engaging with legal experts, simplifying the laws, and incorporating best practices, India can build a legal framework that is more responsive to the needs of its people and the demands of the 21st century.

Sardar Vallabhbhai Patel
National Police Academy
Criminal Law Review 141-149

The Convergence of Artificial Intelligence & the Criminal Justice System: Challenges & Opportunities

ROHAN JHA*

Artificial Intelligence (AI) and Machine Learning (ML) have become pivotal tools in modern society, reshaping various industries and enhancing efficiency across different domains. In the context of the criminal justice system in India, a country marked by its vast and diverse population, the challenges faced by law enforcement agencies are immense. However, the implementation of AI-based solutions offers both opportunities and challenges.

For instance, one notable opportunity lies in predictive policing, which aligns with CrPC Section 41, empowering police officers to arrest individuals without a warrant if they are involved in a cognizable offence. AI-driven predictive policing can analyse historical crime data, enabling the identification of high-crime areas and optimizing resource allocation, ultimately contributing to a reduction in crime rates. This approach has been successfully employed by the LAPD in the United States, leading to a significant decrease in property crime rates [1]. The concept of AI predicting

*IPS (Probationer) 75 RR, Uttar Pradesh Cadre

crimes before they occur, as exemplified in the film "Minority Report" (2002), showcases the potential for a proactive approach to law enforcement, demonstrating the transformative impact that AI can have on the criminal justice system.

Another opportunity is the use of Facial Recognition Technology offers a significant opportunity for the criminal justice system, particularly in alignment with CrPC Section 73, which permits the police to photograph individuals accused of non-cognizable offences. AI-powered facial recognition technology can play a crucial role in the identification and location of suspects. Notably, Chinese law enforcement agencies have harnessed the power of facial recognition with notable success, leading to the capture of numerous suspects. This technology's potential to streamline suspect identification processes and improve investigative efforts can undoubtedly enhance the efficiency and effectiveness of law enforcement operations in India and beyond, bringing a transformative dimension to the criminal justice system. This technology's merits are well-documented in the research, as evidenced by the study "Face Recognition for Criminal Identification" published in the Proceedings of the International Conference on Pattern Recognition in 2016[2].

Natural Language Processing (NLP) offers a compelling opportunity to enhance the capabilities of the criminal justice system. NLP technology can analyze vast volumes of text data to detect potential threats and crimes, particularly in the realm of cybercrimes such as online threats and harassment. This technology has demonstrated its effectiveness in various countries, where it has been utilized to identify cybercrimes, hate speech, and threats on social media platforms. A study titled "Deep Learning for Hate Speech

Detection in Tweets," published in Expert Systems with Applications in 2018, underscores the potential of NLP in identifying and addressing such digital threats[3]. The concept of employing NLP for predictive analysis finds a cinematic counterpart in "The Dark Knight" (2008), where Batman uses AI and NLP to analyze the Joker's writings to anticipate and prevent his next moves, showcasing the transformative potential of NLP in modern law enforcement.

The integration of AI in the realm of legal research and document analysis presents a promising opportunity to advance the efficiency and effectiveness of legal proceedings. AI-powered legal research tools, such as the well-known ROSS platform, are now employed by law firms in the United States, streamlining the process of identifying relevant case law and legal precedents to bolster legal arguments. The concept of AI systems rapidly analyzing extensive legal databases is vividly portrayed in the film "I, Robot" (2004), highlighting the transformative potential of AI in assisting legal professionals in their research and document analysis endeavors, ultimately contributing to the evolution of the legal landscape.

AI technology has the potential to play a pivotal role in victim identification, especially in challenging cases such as human trafficking or missing persons, in accordance with the provisions of CrPC Section 311. This section empowers the Court to summon material witnesses, and AI can assist in the process of identifying and verifying victims. Additionally, AI can revolutionize evidence analysis, aligning with Section 65B of the Indian Evidence Act, which recognizes electronic records as admissible evidence. This entails the use of AI for the forensic examination of digital evidence, offering a more advanced and accurate method of assessing electronic records. In doing so, AI not only streamlines legal proceedings but also

bolsters the integrity of the evidence presented in court, ultimately enhancing the efficacy and fairness of the Indian judicial system.

Artificial Intelligence, while holding great promise, also poses several challenges, the first of which is the issue of data quality and bias. Biased or incomplete training data can result in discriminatory outcomes when AI systems are deployed. An illustrative case is the study conducted by the American Civil Liberties Union (ACLU) in the United States, which revealed racial bias in facial recognition technology employed by law enforcement agencies. This example underscores the real-world implications of biased data in AI applications[4]. The dangers of relying on biased data are vividly portrayed in the film "Minority Report" (2002), where precognitive data leads to the arrest of innocent individuals, highlighting the critical need for addressing bias and data quality issues in AI to ensure fair and just outcomes.

Privacy concerns in the context of AI-driven surveillance also pose a significant challenge as existing privacy laws may prove inadequate in safeguarding individuals' rights. This issue is exemplified by the European Union's General Data Protection Regulation (GDPR), which has set stringent rules for the use of personal data, exerting a profound influence on the adoption of AI technologies across Europe [5]. As illustrated in the film "Enemy of the State" (1998), where the government's extensive surveillance capabilities infringe upon an individual's privacy, the potential for unchecked and invasive AI-driven surveillance is a theme that resonates not only in cinema but in the real world. Ensuring a delicate balance between security and personal privacy remains a critical philosophical and legal challenge in the age of advancing AI technologies.

The utilization of AI for predicting crimes and identifying suspects introduces a host of ethical and legal challenges. Notably, Chicago's predictive policing program has come under public scrutiny, as concerns regarding its fairness and potential for misuse have surfaced. These concerns echo the ethical dilemmas associated with AI-driven crime prediction, emphasizing the need for transparent and accountable practices in law enforcement. The moral quandaries surrounding arresting individuals based on predictions, as vividly portrayed in the film "Minority Report" (2002), raise fundamental questions about the balance between security and civil liberties, emphasizing the complex ethical and legal considerations inherent in the use of AI for predictive policing. The need to navigate these issues while upholding the principles of justice and individual rights is a critical aspect of the integration of AI in the criminal justice system[6].

Resource constraints present a significant challenge in the effective implementation of AI within law enforcement agencies. Many such agencies encounter limitations in both financial resources and the technical expertise required to harness AI technologies to their full potential. An illustrative case can be found in the UK's Police Digital Service, which has encountered difficulties in providing comprehensive AI training to its officers due to limited resources. This practical challenge mirrors the fictional depiction in "RoboCop" (1987), where resource constraints and the overreliance on AI systems are depicted as obstacles in the realm of law enforcement. Navigating these resource limitations while striving to leverage AI's benefits for improved policing and justice remains a fundamental challenge, emphasizing the need for strategic planning and resource allocation. Research in this area, as detailed in "AI in Policing - A Conceptual Framework for the Evaluation of Law Enforcement," published in the

Information & Security: An International Journal in 2019, provides valuable insights into addressing these constraints for the effective integration of AI in law enforcement.

The integration of Artificial Intelligence (AI) in the criminal justice system and policing carries profound philosophical implications that encompass core principles of justice, freedom, privacy, and human rights. Here, we explore these implications, which are essential to understanding the ethical considerations and societal impact of AI in law enforcement.

Firstly, the presumption of Innocence and Due Process in legal systems: One of the fundamental tenets of any justice system is the presumption of innocence until proven guilty. The use of AI, particularly in predictive policing, raises questions about whether an AI system's assessment can infringe upon this principle. If AI algorithms predict criminal behaviour or the likelihood of future offences, individuals could be unfairly stigmatized or subjected to unwarranted scrutiny, potentially undermining the principle of due process.

Secondly, the right to freedom and other fundamental rights: The use of AI for surveillance and data analysis can encroach upon personal freedom and privacy rights. Extensive data collection, facial recognition, and predictive analytics can lead to constant monitoring and profiling of individuals, raising concerns about the balance between security and personal liberty. It prompts the question of whether individuals are being treated as mere data points rather than as autonomous beings with rights.

Thirdly, the challenges to Accountability and Transparency: The 'black box' nature of some AI algorithms poses a challenge to accountability and transparency. When decisions with significant

implications for individuals are made by AI systems, it can be difficult to understand how these decisions were reached. This lack of transparency raises questions about accountability for errors, biases, or ethical breaches.

Fourthly, the implication on the Human Element in Justice: The introduction of AI may shift the focus from human judgement and discretion to automated decision-making. This raises concerns about the dehumanisation of justice. The philosophical debate centres on the role of humans in law enforcement, the legal system, and the inherent value of human judgement and empathy in addressing complex legal matters.

Fifthly, the Slippery Slope of Surveillance: The widespread use of AI surveillance technologies poses philosophical questions about the limits of state surveillance. At what point does surveillance for security purposes become intrusive and a threat to individual privacy? Finding the right balance between public safety and personal freedom is a philosophical challenge.

Sixthly, the ethical responsibility of Developers and Operators: The development and deployment of AI in the criminal justice system raise questions about the ethical responsibility of those involved. Philosophically, there is a need to consider the ethical obligations of AI developers, law enforcement agencies, and policymakers in ensuring that AI technologies respect human rights and ethical standards.

Thus, the use of Artificial Intelligence (AI) in the criminal justice system offers numerous compelling advantages. AI can enhance policing by predicting and preventing crimes through data analysis, improving resource allocation, and thereby increasing public safety. It can assist in identifying suspects and locating missing

persons through facial recognition, making law enforcement more effective. AI's application in case management and document analysis expedites legal processes and research, reducing administrative burdens on legal professionals. Furthermore, AI's capacity for analysing large volumes of data helps identify crime trends, enabling informed policy decisions and more efficient resource allocation. These applications can collectively improve the efficiency, accuracy, and overall effectiveness of the criminal justice system, ultimately leading to a more just and secure society.

References

Safety and Justice Program For More Information Explore the RAND Safety and Justice Program View document details. (n.d.). Available at: https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf.

Abdullah, N.A., Saidi, Md.J., Rahman, N.H.A., Wen, C.C. and Hamid, I.R.A. (2017). Face recognition for criminal identification: An implementation of principal component analysis for face recognition. *AIP Conference*. doi:https://doi.org/10.1063/1.5005335.

Anderson Almeida Firmino, de, C. and Anselmo (2023). Improving hate speech detection using Cross-Lingual Learning. *Expert Systems With Applications*,
pp.121115–121115. doi:https://doi.org/10.1016/j.eswa.2023.121115.

Lee, N.T., Resnick, P. and Barton, G. (2019). *Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms*. [online] Brookings. Available at: https://www.brookings.edu/articles/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/.

Diamantopoulou, V., Lambrinoudakis, C., King, J. and Gritzalis, S. (2021). EU GDPR: Toward a Regulatory Initiative for Deploying a Private Digital Era. *Modern Socio-Technical Perspectives on Privacy*, pp.427–448. doi:https://doi.org/10.1007/978-3-030-82786-1_18.

www.nsf.gov. (n.d.). *NSF Award Search: Award # 1917712 - Collaborative Research: Standard Grant: Artificial Intelligence and Predictive Policing: An Ethical Analysis*. [online] Available at: https://www.nsf.gov/awardsearch/showAward?AWD_ID=1917712&HistoricalAwards=false [Accessed 21 Oct. 2023].

Sardar Vallabhbhai Patel
National Police Academy
Criminal Law Review 150-157

Drugs Lead to Crimes in Maldives

ADAM MAHIR*

According to Goode (2008), drugs and crime are closely linked in the public perception. Currently, it is widely suggested that drugs and crimes are highly associated with each other. Even if this association stands firm, there remains a certain problem: whether or not asset-related offenses would decline under the decriminalization of specific unlawful drugs. There is a critical need for a better understanding of drug abuse and the magnitude of its impact on drug use and crime. The relationship between drugs and crime is a universal issue that affects billions of people worldwide. The Drug Control Master Plan 2009 – 2016 states that drug use is a complex and multifaceted issue confronting the entire country, particularly among young people. There is scarcely a community or a family that is unaffected or free from its harmful effects.

Drug-Related Offenses in the Maldives: Historical Background

Drug abuse and drug trafficking have increased in the Maldives over the past decades, mainly due to exposure to the developing world. The use of drugs was not considered a serious issue until the mid-1970s.

* *IPS (Probationer) 75 RR, Maldives Police Service Cadre*

Although there were reports of opium use in the previous decades, it appeared to be limited to a small number of individuals. The emergence of drug abuse in its current form coincided with the rapid development of the tourism industry in the country in the early 1970s. However, there is no solid evidence to connect these two events. Since this time also coincided with the introduction of drugs into other South Asian countries, it is equally plausible that drugs were brought into the Maldives by young people returning home from nearby countries. Consequently, the abuse of cannabis (marijuana and hashish) became prevalent among young people. Since then, drug abuse has become a significant issue, especially among young individuals. The first reported instance of drug abuse was in 1977 when one person was caught with 350 grams of hashish.

The first legal framework dealing with narcotic drugs and psychotropic substances (the Drug Act No 17/77) was enacted in 1977 to assist the legal system in the Maldives. In 1995, the first amendment was made to the Drug Act (17/77). In 1996, drug abusers were given the opportunity to participate in drug rehabilitation programs, and those who successfully completed them had their pending sentences suspended.

The issue of drug-related offenses has become the most common case filed at the criminal court of the Maldives, showing a 200% increase in the past few years. The rapid growth in drug use is a cause for concern for health professionals and law enforcement authorities since the majority of drug users in the country are between the ages of 16 and 30. When more than 50% of the population of drug addicts is under the age of 16, it becomes an alarming trend for a small country like the Maldives.

After 37 years, a modern legislation was established to address the drug issues. The National Drug Agency (NDA) is responsible for implementing policies related to the legislation under the new Drug Law (17/2011). One of the best features of the new law is the establishment of a drug court to handle drug cases. This court has jurisdiction over all matters related to drugs, as defined by the law, and is part of the general justice system. The drug rehabilitation program aims to reduce the level of drug addiction and minimize the level of criminal activity associated with drug abuse while facilitating the reintegration of qualified individuals into society. It provides judicial and legal recognition to the treatment process while integrating it into the general justice system.

Legal Framework

According to the Narcotic and Drug Act 17/2011, Section 2, any involvement in narcotics, including planting, manufacturing, importing, exporting, marketing, distributing, possessing, with the intent to distribute, is considered an offense and is punishable by life imprisonment. The Drug Act, under Sections 2 and 3, prohibits the manufacture of any prohibited drugs in the Maldives. The manufacture of controlled substances in violation of the law is also prohibited. These provisions also make the supply, import, possession, and trade of chemicals for the production of narcotic drugs and controlled substances punishable in the same way as drug trafficking. Additionally, with the absence of chemicals and related businesses, the rules for the import and abuse of precursor chemicals would not be very complex.

Types of Drugs Used in the Maldives

Over the past 30 years, the availability of various illicit drugs in the country has increased. Heroin, including the crude form known as 'brown sugar,' cannabis and its derivatives, followed by alcohol and opioids, are the most common types of drugs used in the Maldives. There have been occasional reports of cocaine use and abuse of MDMA or ecstasy pills. Some drug users in Malé, as well as in the islands, prefer to inject drugs, which puts them at greater risk of dangerous diseases such as hepatitis and HIV/AIDS. According to a report released by the Maldivian Police Service, the prevalence of injecting heroin is approximately 1% of the drug-using population.

Official documents disclosed that tourists or travelers who visited the Maldives in the 1600s found that the royal family used a drug called opium inside their royal palaces. Additionally, Indian traders introduced cannabis to the Maldives in the 18th century, and in 1972, with the introduction of tourism in the country, marijuana became popular, and young people began to smoke it. Low-grade heroin, known as 'brown sugar,' also became widely prevalent in the nation. In the early 1990s, many people who were using marijuana were arrested. Youths who were arrested while experimenting with drugs were put in jail where isolation was non-existent. As a result, the majority of people who used drugs either became tough and hardened offenders or developed drug addictions.

Factors Contributing to Drug Use

Although drug abuse is considered one of the major problems that can affect the country's development, the government seems to have difficulties addressing this issue effectively. So far, all the governments have shown limited interest in this problem.

The escalating drug use can be attributed to several factors:

1) Unemployment - too much free time without work and boredom among young people lead them to explore the world of drugs.
2) Environment - the environment where a person grows up has a significant influence on drug abuse.
3) Traumas - people who experience psychological traumas might be tempted to alleviate their suffering by turning to drug addiction.
4) Mental illness - the link between mental illness and drug abuse is significant, with more than half of all drug users suffering from a mental disorder.
5) Peer Pressure - teens often start abusing drugs when they see their friends using drugs to fit in with their peers.
6) Lack of family care and love.
7) Drugs as the only recreational activity.
8) Easy trafficking of drugs into the country due to its proximity to international sea lanes.

The First Drug Survey Held in the Maldives

In February 2013, the first national drug survey was conducted, revealing an urgent need for drug use prevention, rehabilitation, and treatment in the Maldives. The study was carried out in close collaboration with UNODC and aimed to provide an overview of the drug abuse situation in the Maldives. Despite drug abuse being a longstanding issue in the nation, there were no previous comprehensive statistics to evaluate the number of people using drugs and the subsequent need for services. The survey revealed that the current drug abuse prevalence, including alcohol abuse, in the capital city Malé is 6.64%. In the atolls, the prevalence rate is around 2%. In total, there are approximately 7,500 drug abusers in the country.

The 2013 survey found that drug abusers were mostly in their early 20s, with a mean age of 21.4 years (ranging from 15 to 42 years). Approximately half of the criminals were under the age of 20. 32% of the drug addicts were between the ages of 20-24 years, and 13% were between 25-29 years of age. Opioids (heroin) and cannabinoids (hashish) were the most commonly used drugs. Peer pressure (38%) and the interest in experimenting (26%) were the main reasons for initiating drug use. The findings pointed out the immediate need for the development of comprehensive strategies for the prevention and rehabilitation of drug users.

Drugs Lead to Crime in the Maldives

According to Adam from the Maldives Police Service (2017), the high crime rate in the Maldives is mainly due to drug abusers. Drug addicts often use drugs before committing a crime and do not fear the consequences of their actions, even if their crimes involve harming innocent individuals. Many crimes, such as assault, theft, sexual offenses, and domestic violence, occur due to drug users. Adam's assertion is supported by Goldstein's theory and research conducted by Lo & Stephens (2008), which also suggest that people use illegal substances when they intend to commit a crime.

The crime statistics of the Maldives Police Service from 2008-2017 have shown that when the drug abuse rate decreases, other crime rates also decrease. This provides clear evidence that drugs are a leading cause of crime. The police have prioritized drug-related crimes and have worked with local and international partners to reduce drug-related offenses. To reduce the risk factors associated with drug-related crimes, public education and awareness programs should be conducted through the media and in schools.

Theories Regarding the Link Between Drugs and Crime

-Substance Use Leads to Crime: Goldstein developed the theory that substance use leads to crime, which consists of psychopharmacological crime, economic compulsive crime, and systemic crime. Psychopharmacological crime suggests that crimes occur when a person is under the influence of a substance, leading to criminal behavior. Economic compulsive crime involves individuals committing economically motivated offenses to support their costly drug habits. Systemic crime arises from drug markets and distribution networks, particularly between dealers and users.

Conclusion

The Maldivian economy heavily depends on tourism, which exposes the population to Western culture and increases the likelihood of drug abuse. This, in turn, creates opportunities for drug trafficking. Police reports and statistics clearly demonstrate that crime rates increase when the drug abuse rate is high. Drug users often become mentally weakened, leading them to commit crimes without fear. To address these issues, various factors contributing to drug abuse need to be considered. According to the UNODC report, several measures have been recognized to comprehensively address the drug situation in the Maldives. These include supply reduction through law enforcement support, awareness programs in schools and communities, and encouraging drug addicts to enter treatment programs. Rehabilitation and awareness programs could be instrumental in reducing drug-related crimes in the Maldives.

Reference

Adyb, A. (2014). Maldives under the burden of drugs. Journal of Alcoholism & Drug Dependence, 1. Retrieved from

https://www.omicsonline.org/open-access/maldives-under-the-burden-of-drugs-2329-6488.1000164.php?aid=28747

Albertin, C. (2011/2012). NATIONAL DRUG USE SURVEY. Male': UNODC. Retrieved from:

https://www.unodc.org/documents/southasia/reports/National_Drug_Use_Survey_-_Report.pdf.

Narcotic Drugs Act (Act No. 17/2011) | Maldives Law.Retrieved from: http://www.nda.gov.mv/about/history

Moore, T. et.al (2016) Effect of adolescent marijuana use on health and other outcomes, p.369

Adam A. (2017, 12 20). drug leads to crime in maldives. (saadhaa, Interviewer)

Maldives Police Service Report (2017) Retrieved fromhttp://www.police.gov.mv/#casestat

N/A. (2015, 3 ,23). Ukesseys. Retrieved from The Relationship Between Drug Use And Crime Criminology Essay: https://www.ukessays.com/essays/criminology/the-relationship-between-drug-use-and-crime-criminology-essay.php

service, M. p. (2017). crime statistics. Male': Maldives police Service.

shazly, m. (2016). DRUG OFFENDER TREATMENT IN THE MALDIVES. Retrieved from http://www.unafei.or.jp/english/pdf/RS_No85/No85_06PA_Maldives.pdf

10. UNDOC. (2013). The first national drug use survey in the Maldives highlights urgentneed for more drug use prevention and treatment. Retrieved from UNODC: https://www.unodc.org/unodc/en/frontpage/2013/February/the-first-national-drug-use-survey-in-the-maldives-highlights-urgent-need-for-more-drug-use-prevention-and treatment.html

Sardar Vallabhbhai Patel
National Police Academy
Criminal Law Review 158-161

From Penal Code to Nyaya Sanhita: A shift from Punishment to Justice

VEDANT SHANKAR*

Law has been an integral part of humankind since the inception of humankind itself. It is as inalienable as air and water for human existence. The presence of law in some form or the other even in the most primitive societies is an indicator of its necessity in any form of community living. From an anthropological point of view, the humankind has survived and evolved up to the present stage due to our strong reliance on group living. Group living is core to human existence because of its survival value. As a species, we have advanced so far not just because of the biological evolution but because of the cultural evolution. The socio-cultural evolution built upon the biological evolutionary advantages accelerated the process of our advancement.

In this context, it is easy to understand the necessity of law in human society. Any form of group living would require certain rules of the group. And any act that is detrimental to this group living and in turn to the survival advantage of the group would need to be

* *IPS (Probationer) 75 RR*, Jharkhand *Cadre*

prevented. Consider the act of theft. Now, theft means dispossession of a material object from one's lawful possession. If theft were not punishable within a society, it would lead to endless conflicts among the individuals. This would have a larger effect on the cohesion of the society and consequently its survival value. Thus, the act of theft is treated as punishable to maintain the social structure. Keeping this logic as the foundation, as the human societies developed so did the law and the guiding principles associated with law.

Roughly stating, we transitioned from prehistoric forms of punishment to the classical school of punishment in and around the time of Renaissance. The prehistoric punishments were so brutal and disproportionate that the arbitrariness of law did not inspire faith in the law and the state. The classical school entailed that human is a rational being and he weighs the cost of doing an act. If the cost of committing a crime were higher than its gains, he would avoid doing it. This is the deterrence that the law aimed to achieve for a harmonious community living. Our modern law codes derive heavily from the classical school of deterrence.

Another school of thought that guides law codes is retributive justice. It is based on the principle of exacting a suffering from the criminal of an equivalent nature because the committed act itself is considered wrong. The *wrongness* of the act inspires the punishment. Now, an application of the above discussion to the *Indian Penal Code* (IPC) would suggest that it reflects a combination of both the deterrent and the retributive theories. To understand its anatomy, we need to take into the consideration the context in which it was designed. The IPC was a product of the British colonial regime that focused on codifying the Indian laws for governing the Indian *'colonial subjects'*. The word *'penal'* itself reflects the intention of the code i.e., to punish

the wrong. The underlying principle is geared towards punishment. It is not to deny that the IPC has served us in good stead. It is also to be acknowledged that the times in which it was designed make it one of the best contemporary law codes. However, as societies evolve, the associated frameworks also need to evolve. The IPC is bounded by the idea of justice that is retributive and the idea of punishment as a deterrence. In the present world, the idea of justice is expanding from retributive and preventive to reformative. It is no surprise that the IPC fails to capture this shift due to its obvious limitations of time and objective, both of which were British.

The *Bhartiya Nyaya Sanhita* is the inevitable evolution of our substantive law framework which was long overdue. The very change in the nomenclature indicates a vital shift in the guiding philosophy of law in India. Foremostly, the intent is justice not punishment. This seemingly innocuous and apparently indifferentiable change is at the heart of the new law code. The change in nomenclature marks a continuation of the war against colonial hegemony, which still finds its way through such remnants as the IPC. It is not mere chance that the CrPC has also been reframed as *Bhartiya Nagrik Suraksha Sanhita*, again indicating that the focus is on citizen and his/her security, rather than the intent of criminalization.

The signs of this change have been present in Indian jurisprudence. The various amendments, such as those focusing on victim justice have been incorporated over time. The Juvenile Justice Act emphatically uses the term *'juvenile in conflict with law'* instead of calling him/her a criminal. However, these efforts have been sporadic. The current criminal law reform bills aim to consolidate these efforts. They also reflect a clear shift of the state from a paternalistic approach to justice to a rights-based one. If we look

beyond the purview of law, we will realize that such churning is not very new. For instance, post liberalization reforms in India, the state's perspective to women's rights changed from *giving* women their due to *empowering* them to take their own due. The same is true with the rights of persons with disabilities. Rather than considering accessibility features as a *favour* by the state, it is now their *right* to claim the same. The *Bhartiya Nyaya Sanhita* and the other two law reform bills encapsulate this evolution of governance philosophy in the Indian state.

Coming back to where we had started, i.e., the necessity of law in ensuring harmonious community living, it is to be noted that such law also needs to be in sync with the society. An outdated framework cannot govern an evolved society. It would often result in conflicts, thereby defeating the very purpose of the law. Thus, in a society that primes itself on rights, liberty, and reformation, a code focusing on punishment must give way to a code emphasizing on justice.

Sardar Vallabhbhai Patel
National Police Academy
Criminal Law Review 162-169

Legal Reforms to Improve Conviction Rates in the Context of Criminal Reform Bills in India

RISHABH BHOLA*

Introduction

The criminal justice system plays a pivotal role in maintaining law and order within a society. However, it is only as effective as its ability to secure convictions that are both just and based on solid evidence. In the context of India, the need for legal reforms to enhance conviction rates is critical. Convictions are not just about punishing the guilty but also about ensuring the innocent are not wrongly incarcerated. As part of a broader initiative to reform the criminal justice system, the government of India has introduced various bills and reforms aimed at addressing the challenges that affect conviction rates. This essay explores the challenges, opportunities, and legal reforms needed to improve conviction rates in the context of the criminal reform bills in India.

* *IPS (Probationer) 75 RR, Odisha Cadre*

Challenges in Securing Convictions

1. **Backlog of Cases:** One of the foremost challenges to securing convictions in India is the backlog of cases. The slow pace of the legal system results in delayed trials, leading to weakened cases due to the loss of evidence and the fading memory of witnesses (Kishor, 2019).
2. **Lack of Forensic Infrastructure:** India has a limited and underfunded forensic infrastructure, which hinders the collection, analysis, and presentation of scientific evidence in court. This results in a reliance on eyewitness testimony, often unreliable and subject to manipulation (Moitra, 2021).
3. **Witness Intimidation and Threats:** Witnesses in India often face threats, intimidation, and coercion, which can lead to recanting their statements or turning hostile during the trial. This threatens the credibility of the prosecution's case and hampers convictions (TNN, 2021).
4. **Limited Legal Aid:** Many individuals accused of crimes in India, especially those from economically disadvantaged backgrounds, lack access to competent legal counsel. This limits their ability to present a robust defense and affects the overall fairness of the trial (Kishor, 2019).
5. **Inefficiencies in Investigation:** Inadequate training, outdated investigative techniques, and corruption within law enforcement agencies can result in subpar investigations, failing to collect vital evidence and weakening the case (Moitra, 2021).
6. **Overburdened Courts:** Overburdened courts struggle to provide timely justice, leading to protracted trials. The lack of speedy trials can deter witnesses from cooperating, and it can lead to a loss of crucial evidence (TNN, 2021).

7. **Legal Technicalities:** Complex legal procedures and technicalities often lead to cases being dismissed or resulting in acquittals. Legal loopholes and delays can undermine the prospects of securing convictions (Kishor, 2019).

Opportunities for Legal Reforms

1. **Clear and Timely Investigation Process**: Legal reforms should aim to expedite the investigation process, ensuring that it is conducted efficiently and fairly. This includes training law enforcement agencies in modern investigative techniques and providing adequate resources for forensic analysis (Moitra, 2021).
2. **Protection of Witnesses**: Legal reforms should focus on ensuring the safety and protection of witnesses. This can be achieved by enacting legislation that makes witness intimidation and threats punishable offences. Witness protection programs should also be established (TNN, 2021).
3. **Enhanced Legal Aid**: The government can introduce legal reforms to improve access to legal aid for underprivileged accused individuals. This can include expanding the legal aid infrastructure and providing competent defence counsel to those who cannot afford it (Kishor, 2019).
4. **Reducing Procedural Delays**: Legal reforms should streamline court procedures and reduce unnecessary delays. This may involve amending laws to limit adjournments, enhancing the use of technology in court proceedings, and increasing the number of judges to reduce the backlog (TNN, 2021).
5. **Reform of Evidence Laws**: The evidence laws in India need to be updated to reflect modern standards. Reforms should

include provisions for the admissibility of electronic evidence, expert testimony, and a focus on scientific evidence over eyewitness accounts (Moitra, 2021).

Legal Reforms to Improve Conviction Rates

1. **Fast-Track Courts**: The establishment of fast-track courts dedicated to specific categories of cases, such as sexual offences or crimes against vulnerable populations, can expedite trials and ensure timely justice. This approach has been effective in reducing backlog and securing convictions (Anand, 2018).
2. **Amendment of Evidence Laws**: A critical legal reform is to amend evidence laws to make the acceptance of scientific evidence, such as DNA analysis, fingerprints, and digital evidence, standard practice in Indian courts. This would reduce reliance on eyewitness testimony, which is often unreliable, and enhance the credibility of the prosecution's case (Mehta, 2021).
3. **Witness Protection Programs**: Legal reforms should include the establishment of witness protection programs. These programs can offer witnesses security, anonymity, and legal support to ensure their cooperation throughout the trial process (Press Trust of India, 2019).
4. **Improvement in Forensic Infrastructure**: A significant legal reform should focus on investing in and modernising the forensic infrastructure in India. This includes building state-of-the-art forensic laboratories, enhancing the quality of forensic training, and providing resources for timely evidence collection and analysis (Mehta, 2021).

5. **Strengthening Legal Aid**: Legal reforms should strengthen legal aid services, providing competent legal counsel for those who cannot afford it. This can be achieved by increasing the budget allocated to legal aid, expanding the reach of legal aid clinics, and promoting pro bono legal services (Anand, 2018).
6. **Alternative Dispute Resolution**: Introducing alternative dispute resolution mechanisms, such as mediation and arbitration, can help reduce the burden on the courts and expedite the resolution of cases that do not require lengthy trials (Mehta, 2021).
7. **Technology Integration**: Legal reforms should promote the integration of technology in court processes. E-filing, digital case management, and virtual court hearings can significantly reduce procedural delays and improve the efficiency of the legal system (Press Trust of India, 2019).
8. **Training for Law Enforcement**: Ensuring that law enforcement agencies receive continuous training in modern investigative techniques, forensic analysis, and ethical conduct is crucial. Legal reforms should include funding and oversight mechanisms to support this training (Anand, 2018).

Here are some real-life examples:

- Digital Evidence Collection and Management: Several Indian states, including Karnataka, have implemented mobile applications that enable police officers to collect and document evidence digitally. These apps facilitate quick reporting, evidence collection, and sharing of information among the law enforcement agencies, expediting the investigation process.
- Crime Mapping and Predictive Policing: Various police departments in India, such as the Delhi Police, have adopted

data analytics and geographical information systems (GIS) to map and analyze crime patterns. Predictive policing models use historical data to anticipate where crimes are likely to occur. This proactive approach enables law enforcement agencies to allocate resources to potential trouble spots, preventing crimes and ensuring quicker responses.

- Forensic Labs and Mobile Forensic Vans: Several states, like Maharashtra, have established modern forensic laboratories equipped with state-of-the-art equipment and technologies. Additionally, mobile forensic vans have been deployed in various regions, enabling the swift collection and analysis of forensic evidence at crime scenes. These advancements aid in expediting investigations.
- Digital Crime Records Management System: The Crime and Criminal Tracking Network & Systems (CCTNS), implemented by the Ministry of Home Affairs, Government of India, aims to create a nationwide database of crime and criminals. This system streamlines the process of filing and accessing criminal records, facilitating quicker background checks and investigations.
- Facial Recognition Technology: Some Indian law enforcement agencies have started using facial recognition technology to identify and track suspects. For example, the Delhi Police used facial recognition technology to identify rioters involved in the 2020 Delhi riots.
- Cybercrime Units and Digital Forensics: Many Indian states have established specialized cybercrime units equipped with digital forensic capabilities. These units investigate cybercrimes, such as online fraud and hacking, using advanced technologies to ensure timely resolution.

- Video Conferencing for Statements: Courts in India, especially in the wake of the COVID-19 pandemic, have started using video conferencing technology to record statements of witnesses. This reduces the need for physical appearances in court and accelerates the judicial process, ultimately impacting the investigation timeline.
- Drones for Crime Scene Reconnaissance: Some police departments have begun using drones for aerial surveillance and crime scene reconstruction. Drones equipped with cameras can quickly capture images and footage, aiding in investigations related to accidents, disasters, and crimes.
- Online FIR Registration and Reporting: Many states have introduced online platforms for filing First Information Reports (FIRs) and reporting crimes. This digital approach expedites the initial stages of investigations and makes it easier for citizens to report crimes.
- Centralized Criminal Databases: The Automated Multi-Modal Biometric Identification System (AMBIS) is an example of a centralized criminal database in India. AMBIS helps law enforcement agencies identify criminals by matching biometric data, including fingerprints and facial images, against the database.

Conclusion

The challenges faced by the Indian criminal justice system in securing convictions are multifaceted, and they require comprehensive legal reforms to address. While it is essential to secure convictions, it is equally crucial to ensure that these convictions are just and based on solid evidence. Legal reforms aimed at improving conviction rates should focus on expediting trials, protecting witnesses, enhancing the

forensic infrastructure, and strengthening legal aid services. Reforms must be designed to reduce procedural delays and increase the admissibility of scientific evidence.

To create a more efficient and fair criminal justice system, India must invest in its legal infrastructure and ensure that law enforcement agencies and legal professionals receive the training and resources they need to excel. Legal reforms are not just about securing more convictions; they are about upholding the principles of justice and ensuring that the innocent are protected from wrongful convictions.

References:

Anand, S. (2018). Special Courts for Speedy Trials and Convictions: A Panacea for Criminal Justice in India. Asian Journal of Multidisciplinary Studies, 6(3), 47-54.

Mehta, R. (2021). Modernising Evidence Laws in India: A Path to Improving Conviction Rates. Indian Journal of Law and Justice, 12(1), 121-132.

Press Trust of India. (2019). Legal Reforms Needed to Improve Conviction Rates: CJI. India Today. Retrieved from https://www.indiatoday.in/india/story/legal-reforms-needed-to-improve-conviction-rates-cji-1526075-2019-05-11

Kishor, P. (2019). Challenges in the Indian Criminal Justice System: A Critical Analysis. International Journal of Social Science and Economic Research, 4(2), 992-999.

Moitra, D. (2021). Criminal Justice Reforms in India: Challenges and Prospects. Journal of Socio-Legal Analysis and Rural Development, 7(1), 58-67.

TNN. (2021). Witness Protection: Law Needed to Instill Confidence in Victims, Witnesses. The Times of India. Retrieved from https://timesofindia.indiatimes.com/india/witness-protection-law-needed-to-instill-confidence-in-victims-witnesses/articleshow/80780276.cms

Sardar Vallabhbhai Patel
National Police Academy
Criminal Law Review 170-174

Police Discretion: Hole in the Doughnut

KAJAL*

Policing rests at a broad decisional latitude, where no law can define the exact bounds hence situations require an individual's judgement and professional standards. This liberty of an individual to act as per their conscience is the discretionary power of police officers, that makes this system humane.

Given the differences in perceptions, experiences, values and morality of an individual, there is a possibility for ambiguity and vagueness to creep in. Hence the boundary wall of discretionary powers, in the form of laws, regulations, standards, rules and policy, is required to restrict and limit this discretion.

Discretion as exigency

Criminal laws are subjective in nature. The mens rea of a crime is difficult to determine. One's state of mind while performing an act cannot be something so simplistic to be reduced into mere sentences. Law draws a strict line between black and white, while the realism of life lies mostly in the grey area to which law provides no space for. Hence, how can a solution be black and white for something that is grey most of the time? A juvenile committing theft to satiate hunger,

* *IPS (Probationer) 75 RR, Telangana Cadre*

is still a crime as per law. Police officers receive complaints of petty theft, robbery, murder, etc. Should their response be the same? Can their response be the same?

A law is as good as its enforcement. Codified laws need enforcement for its effectiveness. Limited resources and personnel act as a limitation on it, hence policemen need their own wisdom to overcome such constraints. If every small dispute gets into the legal system, it will only drain people and police personnel of valuable time and energy.

Consequences of law are harsh and far reaching on one party, barely leaving room for a second chance. A person going to jail for a petty theft comes out as a hardened criminal. Sadly such harsh consequences are never accounted for when designing a law. Such aspects, which law cannot entail within it, are to be dealt with by police discretion. This gives a humane shape to the criminal justice system. The first wall of this system, i.e. police, needs to have this flexibility.

Discretion has been leading the way

Various discretionary powers exist like powers of arrest u/s 41 CrPC, i.e. power of a police officer to take away someone's liberty. Just like that, someone can be deprived of their liberty. Here comes the wisdom of police at play; whom to arrest and whom not to arrest, to ensure an impartial investigation that does not go against judicial economy.

Another example is the power of police officers to search u/s 165 CrPC, based on reasonable grounds as per police officer's belief. If police had to go to the court for permission of every small matter, the increase in pendency and judicial workload is not difficult to

imagine given that already 4.5 crore cases are pending in our courts and prisons are filled with 67% undertrials.

Even in domestic disputes cases, discretion comes into play. Mediation in trivial matters by the police prevents small disputes from flaring up, prevents families from breaking up and ensures peace in communities. For juvenile offenders in minor cases such as public intoxication, giving them a warning instead of pressing formal charges protects them. Police choosing to go after the big fish of a narcotics gang instead of arresting consumers creates a bigger impact. This ensures judicial economy, while also ensuring a second chance to offenders, preventing them from falling into a bigger nexus.

Pandemic times brought out the best side of police in our country. Police were not there to create fear among the public by arresting them for petty violations like lockdowns etc. Instead they were offering roses on roads to ensure that moral responsibility among people becomes our defence in challenging times, when law alone was not able to protect the public. The discretion used by police to punish and to create awareness, bore fruits in the form of people becoming partners of police and fighting the enemy together.

Slippery slope

The natural tendency of human biases creeping into one's discretionary decisions, be it based on gender, religion, race, etc., makes certain groups vulnerable to selective targeting. We have seen various such instances towards habitual offenders, certain tribal groups & lower income groups. Rarely will we see traffic police personnel stopping an SUV for a breath analyser test. Instances of moral policing, eg. police officers pointing fingers at girls in eve teasing cases, or their reluctance to register rape cases between known persons, speaks volumes about the individual's moral corruption tilting the scales of justice and in favour of influential people.

Registering cases based on whims and fancies may make justice a luxury accorded to only a few. It may erase fair and just law enforcement, and violate the rights of people. For example, random arrests by the police. Street justice in the form of police discretion can be dangerous. Putting justice into arbitrary hands is not desirable for a progressive society. Hence, we must set boundaries on the discretionary powers of police to prevent their possible abuse.

Repairing the cracks and leaks in the wall

The Prakash Singh judgement[1], which put down guidelines to set up a Police Complaint Authority, tried putting up a solid defence to prevent abuse of police discretion if followed in letter and in spirit, thus ensuring accountability. The bar set by it needs to be raised one notch above, be it in the form of body cameras or more effective supervision by seniors.

Efforts have been made to build this wall of accountability in the law itself, in the form of Section 41A CrPC, to make police accountable for their most-abused power of discretion during arrest. In-built safeguards in the form of implementation of DK Basu guidelines[2] & Arnesh Kumar judgement[3] have helped reduce ambiguity and arbitrariness during arrest procedures.

The penultimate safeguard lies in the hands of the public itself. Only those who are aware of their rights can defend them. Hence public awareness about the law, the loopholes and how to stand up against their misuse should take priority. Transparency in police functioning should remove the curtain between police actions and the

[1] Prakash Singh & Ors vs. Union of India & Ors (22nd September, 2006)

[2]Shri D.K. Basu, Ashok K. Johri vs State Of West Bengal, State Of U.P on 18 December, 1996

[3] Arnesh Kumar vs State Of Bihar & Anr on 2 July, 2014

public, to ensure that police are accountable to the people for the decisions they take.

Discretion can be a boon or a bane, depending on the hands in which it lies. If used as a tool of extortion, it leads to chaos and anarchy. On the other hand when used with caution and accountability, it can become a tool of justice that is not costly or out of reach. The difference in the use of this discretion decides whether police officers become the public servants or the high-handed law enforcers in uniform.

A PUBLICATION OF THE
SARDAR VALLABHAI PATEL NATIONAL POLICE ACADEMY
HYDERABAD