THE INTERFACE BETWEEN LAW AND TECHNOLOGY

PUBLISHED BY

Navrachana University in association with Gujarat National Law University

The Interface between Law and Technology

Edited by

1. Dr Sujatha S Patil (NUV)
2. Dr. Thomas Mathew (GNLU)
3. Mr Navin Sinha(NUV)
4. Ms Chandrika Tewatia Raj (NUV)
5. Ms Heena Goswami (GNLU)
6. Ms Madhura Thombre (NUV)
7. Dr Meghna Vyas (NUV)

ISBN 978-81-950434-4-6

ACKNOWLEDGEMENT

As we ready ourselves to peruse the content of the book, we would be failing in our duty if we do not acknowledge the contribution of all those who were directly or indirectly connected with the publication process. At the outset, we would like to acknowledge the organisers and participants and guests of the International Conference on The Interface between Law and Technology. The Conference, in more ways than one, was the main reason that we were able to compile all the insightful chapters in the book.

We are also grateful to Prof (Dr) S. Shanthakumar, Director, Gujarat National Law University, and the team of Centre for Law and Technology for associating with us as knowledge partner and helping us with the publication process. We are also equally grateful to the management Navrachana University for backing us up at all the right times. Our thanks are also due to Dr Meghna Vyas for helping us acquire the ISBN. Without her timely intervention the whole process would have collapsed. Our thanks are also due to all the students who helped us immensely in the compilation chapters and working their magic through various software as a part of the publication process.

The days leading to the publication were often complicated sometimes really frustrating. It was during those days that we had the guidance of several people including Prof Nilay Yagnik, Provost, Navrachana University, Dr. Hitesh Bhatia, Associate Dean, School of Business and Law and Dr. Sujatha Patil, Principal Law Program. School of Business and Law. We are indeed grateful for their guidance and support throughout those hard times. We would also like to thank Prof Benjamin G. Davis who addressed the Conference as one of the key note speakers and very kindly helping us in writing the preface of the Book.

Finally, we would also like to express our gratitude to all the nameless forces that was directly or indirectly connected with the publication process.

PREFACE

As we continue adapting to the technology wave that has accelerated over the past 50 years, this conference and these papers come at a very opportune time for reflection. As technology finds its way - like water in a flood - into every aspect of society, it is no longer possible to say no to technology. On the contrary we have to think deliberately and carefully about how that technology comes into the aspects of what we term law. It is important to make sure that the procedural fairness that is the hallmark of any democratic legal process is maintained and even possibly augmented with the assistance of these technologies. Whether in accelerating repetitive tasks in the legal field or helping with more creative and innovative aspects of law practice, the technology must be an aid. Without a conscious deliberate effort to think through the implications of any choice of approach to technology, we risk inadvertently introducing bias and false results that gain more legitimacy because they come from what an algorithm or machine learning has generated. This book helps us remember that Artificial Intelligence is merely a human creation and that human frailties can risk being poured into the manner of operation of the expert system. We are called to be vigilant in our embrace of technology to make sure that we do not by enthusiasm create something that does not preserve rights but does wrongs – in this case we might call them algowrongs. If that happens, we will find us not confronted with technology but with having been duped by what we thought would help us: what has been called tricknology. Blessed with the faith that humans can chart a course that finds assistance from technology without becoming beholden to the same technology, I hope that you enjoy reading the excellent contributions in this work to spur your own reflection and action.

Sincerely,

Benjamin G. Davis
Professor Emeritus of Law
University of Toledo College of Law Toledo,
Ohio USA

MESSAGE FROM THE PROVOST

One of India's most respected Industrialists, Mr.Ratan Tata, is known to have said "*None can destroy iron , except its own rust. None can destroy a person except the person's own mind-set*"

We are living in a time where change is so rapid. Technology is driving this change at a speed never before seen. New technologies are coming up, affecting all aspects of our life - Education, Healthcare, Commerce, our lifestyle and relationships, the way we communicate, the Entertainment options available and the Society as a whole. Therefore, , it is very important for humans not only learn to adapt to these technologies , but also use these technologies to be good humans. And this is where Law comes in. The purpose of Law is to help make a person a good citizen. Therefore, Law and Technology should go hand in hand. But the challenge that is always there is that technology changes too rapidly bringing with it newer problems. The Law is often behind the rapid pace of change of technology and its applications.

This International Virtual Conference on the Interface between Law and Technology has therefore been organised jointly by Navrachana University and the Gujarat National Law University to address issues which will help this divide. This Conference has more than ten sub themes which include areas ranging from the Constitution and Technology, IPR and Technology, Legal Issues in Artificial Intelligence , Technology and Health Law , Technology in Legal Education and such areas. Speakers and Papers were received and presented from all over India and around the World. There are several practicing Legal luminaries and Industry experts too who gave their talks and views at the Conference. This book is a compilation of these papers and will serve as a good reference to Academicians, students, and the practicing legal fraternity to be updated on this very important and relevant aspect of the Law and Technology.

Dr.Nilay Yajnik
Provost,
Navrachana University

GENERAL CONTENTS

Chapters **Pages**

i. Introduction ……1-3

ii. Technological issues under Environment Law ……..….....4 - 71

iii. Legal issues under Artificial Intelligence …….. 72-175

iv. Commercial Law and Technology: E-Contracts, Cryptocurrency, Ecommerce, Taxation, International Trade etc. ……..….. 176-200

v. IPR and Technology ……... 201-225

vi. Impact of Technology on Legal Education & Profession……..……. 226-245

vii. Cyber-crime under AI…….…..... 246-290

viii. Constitutional Perspectives in Technology…….…… 291-312

ix. Biotechnology and Law……...…….. 313-339

x. Jurisprudential issues in Cyber Space……..... 340-348

ARRANGEMENT OF CHAPTERS

CHAPTER I

TECHNOLOGICAL ISSUES UNDER ENVIRONMENT LAW

PAGE

1. The Fault in Our Artificial Stars: Efficacy of Satellite Surveillance Systems in India's Conservation Efforts…… 4

2. Technological Effects on Right To Privacy With Special Reference To Media Trial…… 19

3. Sustainability Through Green-Buildings: A Study With Respect To Real Estate, Environmental Protection, And The Sdg's…… 28

4. E-Waste A Catastrophe Lurking Around The Corner: Insights Into It's Impact On The Environment And Prevailing Legal Regimes In India……..…… 36

5. Technological Perspectives Of Media Law……..…….. 46

6. Telemedicine and Data Privacy Of Patient: Sine Qua Non For Reforming Health Services…….. 55

CHAPTER II

LEGAL ISSUES UNDER ARTIFICIAL INTELLIGENCE

7. Reviewing the Legal Considerations Of Artificial Intelligence In India……. 72

8. Legal Issues Under Artificial Intelligence ……..…… 81

9. Assessing The Probability Of Artificial Intelligence In Criminal Investigation……. 96

10. How AI can improve the Justice Delivery System in India …… 105

11. Deliberating the Science of Artificial Intelligence with focus on the

Legal Issues Pertaining with it……. 117

12. Deciphering The Dilemma Of Ownership And Liability

In the Realm Of artificial Intelligence ……. 127

13. Intellectual Property Rights And Software Patent: A Problem Of Innovation…….. 142

14. Fixing Liability For Automated Vehicle And Protecting

Innovative Automobile vi Technology In Indin…….....153

15. Smart Laws For Smart Society And Smart Technologies: Need Of The

Hour……..…….. 163

CHAPTER III

COMMERCIAL LAW AND TECHNOLOGY: E-CONTRACTS, CRYPTOCURRENCY, E-COMMERCE, TAXATION, INTERNATIONAL TRADE ETC

16. ROLE OF LAW IN E-COMMERCE ACTIVITIES…… 176

17. E-Commerce Challenges And Their Solutions Under Consumer

Protection Act, 2019 And Consumer Protection (E-Commerce) Rules, 2020…...……187

CHAPTER IV

IPR AND TECHNOLOGY

18. Role Of Intellectual Property In The Fashion Industry: A Legal Perspective……. 201

19. Digital Era And Coppyright Issues: An Analysis……... 215

CHAPTER V

IMPACT OF TECHNOLOGY ON LEGAL EDUCATION & PROFESSION

20. Impact Of Technology On Legal Profession And Education In India: An

Overview……. 226

21. E-Courts: Start, Pandemic Response And Future …… 237

CHAPTER VI

CYBER-CRIME UNDER AI

22. Nth Room Case And Fight Against Online Sexual…….. 246

23. CYBER TERRORISM: A Global Security Threat……... 257

24. The Curious Case Of Modern Cyber Warfare: Issues And Challenges……... 269

25. Social Media And The Emerging Dimensions Of Cybercrime In India…….. 278

CHAPTER VII

CONSTITUTIONAL PERSPECTIVES IN TECHNOLOGY

26. Subhranshu Rout At Gugul V. State Of Odisha – An Insight Into The

Right To Be Forgotten As A Fundamental Right In The Cyber Realm……. 291

27. Censorship On Intermediaries: A Solution To Stop Misuse

Of Social Media? 304

CHAPTER VIII

BIOTECHNOLOGY AND LAW

28. From Test Tube Babies To Human Clones: Exploring Red Biotechnology

From The Lenses Of Law…….……. 312

29. Research Paper On Brain Mapping (Bmt) Or P300 Test (Forensic Science)….. 328

CHAPTER IX

JURISPRUDENTIAL ISSUES IN CYBER SPACE

30. Ethical Issues In Cyberspace: A Jurisprudential Approach……. 340

INTRODUCTION

Navin Sinha[1]

There is no gainsaying that advancements in science and technology have had a massive impact in the advancement of the law and legal techniques. This is no better exemplified than by our advancements in the field of forensic technology. Indeed, advancements in forensic technology have highly optimised our investigative tools making criminal investigation more potent and penetrative. This is especially true in the case of DNA profiling. The use of DNA samples has proven to be an effective investigative tool and this technique has successfully aided in identifying "unknown victims, suspects, and serial offenders" and in some case it has also helped in releasing wrongfully charged or convicted individuals.[2] The fact is contemporary DNA profiling methods are based on scientifically approved research standards.[3] Thus, the DNA backed evidence are not only accurate but at times the only method to come to a conclusion. There are caveats, however, and even the most advanced scientific procedure can mislead us in our search for justice.[4] While the caveat may apply to overreliance of on technologies for dealing with our legal issues, it also equally applies to wrongful or erroneous use of technology for dealing with legal issues. History is replete with examples of how the erroneous use of technological tools have impacted our fundamental freedoms including life.[5] In this context Petherick observes that in most cases this occurs,

> when experts do not avail themselves of all available evidence, when they are oblivious or unaware of evidence that exists, when experts are not aware of their own shortcomings, or where bias or cognitive distortion taint the expert's opinion, even in cases where the evidence may be pristine or voluminous.[6]

---

[1] Asssitant Professor, Navrachana University

[2] Aaron Opoku Amankwaa and Carole McCartney, 'The Effectiveness of the Current Use of Forensic DNA in Criminal Investigations in England and Wales' n/a WIREs Forensic Science e1414 <https://onlinelibrary.wiley.com/doi/abs/10.1002/wfs2.1414> accessed 7 July 2021.p 2

[3] ibid.

[4] Ventana al Conocimiento, 'The Failures of Forensic Science' (*OpenMind*, 30 January 2017) <https://www.bbvaopenmind.com/en/science/scientific-insights/the-failures-of-forensic-science/> accessed 7 July 2021; 'Why Forensic Science Is in Crisis and How We Can Fix It | World Economic Forum' <https://www.weforum.org/agenda/2019/09/why-forensic-science-is-in-crisis-and-how-we-can-fix-it/> accessed 7 July 2021.

[5] Wayne Petherick, Errors and Failures in Forensic Practice in Elisabeth Vanderheiden and Claude-Hélène Mayer (eds), *Mistakes, Errors and Failures across Cultures: Navigating Potentials* (Springer International Publishing 2020) 475

[6] ibid.

Introduction

Contemporary time is the time of technological advancements; and even as we marvel at how this has affected our understanding of law we need to understand this is not an easy relationship. The union between the two, besides the obvious advantages, comes with a fair share of warning too. Indeed, it wouldn't be wrong to say that the path they present is both dangerous and advantageous too. There are pitfalls to manoeuvre, impediments to overcome and sometimes temptations to resist. And moreover, there are ethical issues to consider as well. As observed by the SC in *Anuradha Bhasin v Union of India*[7]

> Law and technology seldom mix like oil and water. There is a consistent criticism that the development of technology is not met by equivalent movement in the law. In this context, we need to note that the law should imbibe the technological development and accordingly mould its rules so as to cater to the needs of society.[8]

The present society, in part, is a creature of our technological assertions and law's effort to control it. Law is in a state of constant flux with technology and this in turn has given rise to numerous issues. While some issues are relatively stable (in terms of its impact in the society), others can have far-reaching implications and demands creative solutions.

The present anthology is a collection of several essays in which various scholars have discussed these issues at length and suggested their solutions as well. These essays have been selected from a series of papers that were presented at the International Conference on Law and Technology at Navrachana University on 30 January 2021. For the convenience of the readers, the anthology is divided into several sections each relevant to the issue that will be discussed therein. The issues are diverse in nature and comprises of varied concerns like IPR and technology, technological advancements and environmental law, legal issues under artificial intelligence, commercial law and technology, technology and education, cybercrime and jurisprudential and philosophical implications of technology. Technological progress is not only inevitable but necessary as well. We stand at a paradoxical time today. While society demands technological progress in every aspect of their life, they also rely on legal institutions for harnessing its potential for harm. While

[7] 'Anuradha Bhasin vs Union Of India on 10 January, 2020' <https://indiankanoon.org/doc/82461587/> accessed 7 July 2021.
[8] ibid 24.

not presently a crisis, but our inability to find timely solutions (legal or otherwise) to techno-legal challenges can soon develop into one. The present anthology is an effort towards the end.

THE FAULT IN OUR ARTIFICIAL STARS: EFFICACY OF SATELLITE SURVEILLANCE SYSTEMS IN INDIA'S CONSERVATION EFFORTS

Shubham Prakash Mishra[1] and Shambhavi Thakur[2]

ABSTRACT:

In modern times, technology has intersected every field of study and research. Environmental law has thoroughly integrated technology in conservation and protection efforts under various national and state legislations. Under legislations such as the Wildlife Protection Act and the Forest Rights Act, satellite imagery is used for data collection to help the authorities study and analyse the need for protection in certain areas. It is labour free and cheaper compared to the infield, manual counting and surveying method. The authorities rely on it to take environmentally directed actions such as reservation of forests, preservation of species, or eviction of forest dwellers. The courts too have often relied on it to decide whether traditional forest dwellers adversely impact the forest and the wildlife and whether they should be evicted and relocated. Their popularity can be attributed to the fact that science and technology enjoy the benefit of objectivity. Yet, as the Gujarat High Court noted in Action Research In v. the State of Gujarat, technologies such as satellite imagery are not infallible. It faces issues such as lack of clarity due to cloud cover, air pollution, and other externalities. Moreover, its interpretation requires skillsets and institutions which are not yet widely accessible or adequate. There are hurdles such as lack of access to resources by the stakeholders, insufficient training of the authorities, and an absence of a screening authority. The indiscriminate use of satellite imagery by the authorities has adverse implications for the forest-dwelling communities. It is used in reserving forests which leads to the large scale displacement of these communities, thereby substantially interfering with their traditional and cultural rights. In this paper, we will trace the use of satellite imagery by the courts in environmental cases. We will then analyse its evidentiary value and provide recommendations for improving its application.

I. INTRODUCTION

Renaissance was a period of enlightenment because its advocacy of science offered reliability and objectivity, a truth devoid of biases.[3] The modern litigator has artfully used

[1] 3rd Year BALLB Student, Jindal Global Law School
[2] 5th Year BALLB Student, Jindal Global Law School

this to advance the reliability of technology by tethering it to objectivity. It is important to acknowledge the critical role played by satellite data around the globe in addressing the issues of climate change and ozone depletion.[4] International bodies such as the United Nations, Intergovernmental Panel on Climate Change (IPCC), and National Aeronautics and Space Administration (NASA) have consistently used it to rally nations together for addressing the concerns posed by first, ozone depletion, and now climate change. NASA frequently collaborates with various countries to provide data on weather and ocean pattern studies.[5] Closer to home, in India, the Environment Pollution Control Authority (EPCA) has used satellite data to monitor air pollution in Delhi.[6] It has also proven to be a useful tool in river valley litigations. Several disputes surrounding the Narmada valley have extensively used this remarkable invention.[7]

Technologies with broad applications and straightforward human collaboration have provided a significant vantage point. However, the ones situated in the complex web of human interactions need a closer critical appraisal and a reconsideration. One such example for the latter use is satellite data for forest conservation. The technological advancement in the field of satellites and image capturing has induced a shift from the traditional ways of collecting evidence for reserving national parks and forests. State agencies rely heavily on satellite imagery as one of the most commonly used methods of data collection. Satellite imagery costs far less than a physical survey and is also less time-consuming. The State exercises its powers under various legislations to collect evidence, which helps in identifying an area for conservation.

Most of these legislations lack technologically informed implementation. Due to this, there is excessive reliance on low quality, old, and misinterpreted satellite imageries and remote sensing technology. Several studies in various jurisdiction have shown that satellite

---

[3] A.C. Crombie, 'Science And The Arts In The Renaissance: The Search For Truth And Certainty, Old And New' (1980) 18 History of Science.

[4] Rosamund Pearce, 'Satellites and Climate Change: how Scientists are using observations from Space to Study the Climate System' Carbon Brief (2016) https://www.carbonbrief.org/interactive-satellites-used-monitor-climate-change#:~:text=A%20geostationary%20orbit%20allows%20satellites,of%20ground%20with%20each%20orbit.

[5] 'Rising Waters: How is NASA monitoring Sea Level Rise' NASA. https://www.nasa.gov/specials/sea-level-rise-2020/

[6] Sandhya Dangwal, 'Delhi air quality: Satellite imagery to be used by EPCA to identify pollution hotspots in Delhi-NCR', India News (2017). https://www.india.com/news/india/delhi-air-quality-satellite-imagery-to-be-used-by-epca-to-identify-pollution-hotspots-in-delhi-ncr-1939546/

[7] *Narmada Bachao Andolan v Union of India*, W.P. (C) No. 319 of 1994.

imagery can be flawed due to various reasons like pollution, cloud cover and other atmospheric disturbance. Furthermore, it is often the case that the pixels are distorted which leads to an inaccurate count of the trees or wildlife in herds. Therefore, the Forest Rights Rules (the Rules)[8] reiterate the cautious use of satellite imagery and that it should not replace the traditional surveying and mapping of the forests and animals.[9] Even if we consider that satellites are reliable for counting trees and mapping forests, they are still incapable of giving accurate data on wildlife.[10] The State incorrectly uses satellite imagery to protect the forest covers, evicting the forest-dwelling communities in the process. Resultantly, these communities, which are minorities and mostly illiterate, are deprived of their rights. The key lies in carrying out surveys and mapping the forest manually and then supplementing it with the satellite imagery. In this paper, we argue that while Satellite Imagery is an indispensable tool in environment protection, its current application is unsuitable for India's Wildlife and Forest Conservation Efforts. Firstly, the technology is in its nascent stage and faces issues such as lack of clarity and other externalities. Secondly, the agencies rarely use the necessary skillsets in its interpretation. This leads to instances of faulty data and unscientific usage.[11] Thirdly, despite such insufficiencies, the agencies choose to rely solely on satellite imagery. This is contrary to the legislation and common practices in this regard all over the world. All of this leads to a faulty implementation and the illegal use of the technology.

We have primarily considered the use of satellite data to resolve human-wildlife conflict while mainly focusing on the Forest Rights Act (the FRA).[12] In Part II of the paper, we highlight the intersection between Technology and Legislations. Legislations lack the scientific advancement and leave a void when it comes to evidence collection for preserving flora and fauna. Due to this, the State conveniently relies on cheap and labour free method of remote sensing and satellite imagery for evidence purposes. In Part III of the paper, we analyse the evidentiary value of the satellite data and its misapplication. The evidentiary requirement under the various Environmental Acts is similar. Firstly when dealing at the quasi-judicial level, the authorities must use at least two pieces of evidence including satellite imagery. Secondly, when the cases are dealt with by the higher courts, the courts must be

[8] Scheduled Tribes and Other Traditional Forest Dwellers (Recognition of Forest Rights) Rules, 2007.
[9] Howard Latin, Gary Tannehill, Robert E. White, 'Remote Sensing Evidence and Environmental Law', CLR December (1976)
[10] Perras, M. & Nebel, S., 'Satellite Telemetry and its Impact on the Study of Animal Migration' 3 Nature Education Knowledge 12, (2012)
[11] *Action Research In v State of Gujarat*, W.P. No. 100 of 2011.
[12] The Scheduled Tribes and other Traditional Forest Dwellers (Recognition of Forest Rights) Act, 2006

mindful of the fallibility of the data. However, the same is not followed in practice, which leaves a huge implementation gap. In Part IV, we offer recommendations based on successful domestic practices.

II. INTERSECTION OF TECHNOLOGY AND LEGISLATIONS

Governments and the State rely primarily on evidence to determine which parts of forests, species, or other flora and fauna to be conserved. The legislations which vest the power to the government to reserve a certain area and species are the Indian Forest Act 1927[13], The Wildlife Protection Act 1972[14], the Forest Rights Act 2006[15] and their instrumentalities. Unfortunately, most of these legislations are severely outdated and have vague notions of data collection which form substantial evidence during the claims process. This is mostly because the analysis of individual trees based on remote sensing images is a complex problem. What is detected as a single object may represent a separate branch or even a group of trees.[16] Most commonly, satellites that capture large forest areas use image technology and the images are made of fine pixels. The pixels of current coarse spatial resolution sensors typically represent a ground area of 1 km and so the vast majority of pixels will cover a ground area with two or more land cover classes mixed pixels cannot be accommodated or appropriately represented in the conventional 'hard' techniques used widely in remote sensing. Consequently, this results in a classification error of up to 50% with the extent of forest cover underestimated, resulting in an overestimation of deforestation rate.[17] one-to-one (canopy to-canopy) assessment is very challenging for tree crown change due to both systematic and non-systematic errors that occur during the acquisition of satellite images over different periods.[18]

Satellite Imagery Technologies in India and Their Pitfalls

Aerial photography of forest and tree covers started roughly a century ago in many western countries. India was one of the later countries to join the list. The multispectral data obtained from satellites like LANDSAT were used to study broad forest features either by

[13] Indian Forest Act, 1927.
[14] Wildlife Protection Act, 1972.
[15] The Scheduled Tribes and other Traditional Forest Dwellers (Recognition of Forest Rights) Act, 2006.
[16] Marilia Ferreira Gomes, 'Detection of Tree Crowns in Very High Spatial Resolution Images Intechopen' (2015)
[17] D.S. Boyd1, F.M. Danson, 'Satellite Remote Sensing Of Forest Resources: Three Decades Of Research Development' PPG 7 (2005).
[18] Kabir Uddin*, Hammad Gilani, M. S. R. Murthy, Rajan Kotru, and Faisal Mueen Qamer, 'Forest Condition Monitoring Using Very-High-Resolution Satellite Imagery in a Remote Mountain Watershed in Nepal' MRD (2015).

visual interpretation of data in the form of imageries or by computer analysis of the multispectral data. However, the limitations are low spatial resolution and lack of stereo coverage[19] However with the increasing presence of technology in every realm, more technologically advanced satellites are being currently used including third party applications like Google Earth. Due to the efficiency and success rate of the LANDSAT series of satellites, NASA is planning to send LANDSAT-9, later this year. However according to a report, since 2003, a mechanical fault in the Scan-Line Corrector (SLC-Off) of the Landsat-7 satellite resulted in a 22–25% data loss in each image.[20]

A fundamental problem faced by researchers studying forests is the lack of appropriate ground data that can be brought together with the remotely sensed data.[21] The state cannot rely on GPS and satellite imagery because the problem with GPS systems is that they do not function if the signal path is blocked (e.g., by dense forest canopies or natural topography), nor do they transmit/receive signals underwater. Even when a physical GPS transmitter is attached to an animal, the weight of the transmitter has to be less than 5% of the animal's body mass. Further, The smallest satellite transmitter commercially available weighed 9.5 g, which means that animals that weigh less than 240 g cannot be tracked with current satellite technology.[22] This excludes about 81% of all bird species and two-thirds of the world's mammals from satellite tracking. Moreover, the expense of the flawed technology is too much, the cost of these telemetry devices is quite high, more than $3000 US.[23] Although some might consider the cost of raw satellite data meagre, the image processing cost and expert fees for interpretation are a major concern for most litigators especially the marginalised.[24]

Improper legislation or application of scientific data collection is most dangerous to the marginalised forest-dwelling communities which are evicted in name of conservation of flora and fauna. In a circular released in 2017, the National Tiger Conservation Authority

[19] Madhvan Unni 'Forest survey and management using remote sensing' PIAS 6, p. 209-231 (1983).
[20] Lahiru S. Wijedasa 'Overcoming Limitations with Landsat Imagery for Mapping of Peat Swamp Forests in Sundaland' R.S. (2012) doi: :10.3390/rs4092595
[21] D.S. Boyd1, F.M. Danson, 'Satellite Remote Sensing Of Forest Resources: Three Decades Of Research Development' PPG 7 (2005).
[22] Perras, M. & Nebel, S. 'Satellite Telemetry and its Impact on the Study of Animal Migration' 3 Nature Education Knowledge 12, (2012).
[23] Ibid.
[24] Sharon Hatch Hodge 'Satellite Data and Environmental Law: Technology Ripe for Litigation Application' *2* PELR (1997).

(NTCA) ordered the directors of all tiger reserves to refrain from recognising the rights of forest dwellers within critical tiger habitats.[25] This is one of the examples when the indigenous population and the forest-dwelling community is evicted and the authorities cite maps and evidence collected by faulty imageries. On the contrary, numerous surveys and case studies have shown that the forest-dwelling communities and indigenous population have contributed to the forest growth by their ancient wisdom and knowledge.[26] Additionally, a lack of redressal mechanism and unawareness in these communities takes their basic rights away. We will now analyse the primary legislations which deal with evidence collection and try to understand their faulty mechanism in detail.

Indian Forest Act, 1927

The Indian Forest Act (the IFA) is the primary legislation which defines forests and lays down the procedure for the government to protect the same. However, this Act is a part of the long list of colonial legislation which has outlived their duration. The process, definitions and redressal mechanism in the IFA is vague and outdated. Section 35[27] of the IFA provides the government with the power to protect forests for special purposes even if that land is not a property of the government. This process is usually done with evidence collected from the local gram panchayat, maps and surveys. After the introduction of remote sensing and image capturing technology, satellites and drones are relied on. The Act is silent on data collection and minimum evidence to be procured to declare a certain area as reserved. Although the Act has gone through many amendments since its inception, it has not caught up with the modern technological advancement in its various fields.

Wildlife Protection Act, 1972

The Wildlife Protection Act is also a half a century old Act which is technologically outdated. It vests immense discretionary power in the collector[28] who identifies the wildlife species based on vague evidence. The collector acts on the behalf of the state government which has the power to declare a certain area of a forest as national parks and sanctuaries. This power is granted in Section 35[29] of the Act. Section 19[30] of the Act vests extreme

[25] The Wire 'Criminalising Forest-Dwellers Has Not Helped India's Forests or Wildlife. It's Time for a New Deal' https://thewire.in/environment/forest-rights-dwelling-communities
[26] C. Madegowda Economic and Political Weekly Economic and Political Weekly Vol. 44, No. 21, 2009, p 65-69
[27] Indian Forest Act, 1927, Section 35.
[28] Wildlife Protection Act, 1972.
[29] Wildlife Protection Act, 1972, Section 35.

discretionary power with the collector to decide on the rights of the forest-dwelling communities. This leads to discrepancies in vesting of traditional rights. Section 23[31] talks about the power of the collector to identify, survey or map a land to be protected as national parks. Like the IFA, this Act also does not clearly describe the type of evidence collected therefore lacking in the advancements. The immense power with the collector with vague and ambiguous guidelines on evidence collection leads to a problematic situation not only for the forest-dwelling communities but gives an inaccurate result of the forest area. Although satellites and images are used in drawing maps and identifying big mammals, they fall behind to capture smaller animals and lightweight birds. Therefore, an extensive ground survey is necessary to advance satellite imagery.

Forest Rights Act, 2006

Being a relatively new Act, the FRA has inculcated scientific and technological methodologies like satellite imagery. However, this part will only focus on the evidentiary value of the FRA which deals with satellite imagery. The FRA aims to recognize and vest the forest rights and occupation in forest land in Forest Dwelling Scheduled Tribes (FDST) and Other Traditional Forest Dwellers (OTFD) who have resided in such forests for generations. Initially, the British had arbitrarily demarcated and reserved forest land, notwithstanding the people already inhabiting such lands. Then after independence, there was a string of legislation such as the Forest Conservation Act,[32] and judgements which relocated forest-dwellers for development and industrialization needs.[33] In the landmark judgement of *T.N. Godavarman Thirumulpad v. Union of India,* the Supreme Court held that the FCA applied to all forest area, irrespective of ownership. [34] Resultantly, the forest-dwelling communities became encroachers instead of owners. Thus began the first wave of mass-eviction of forest-dwelling communities.[35] The Forest Rights Act is a landmark piece of legislation which promises to undo the historical injustice meted out to forest-dwelling communities by recognising their rights over the land, forest and natural resources that they conserved and

[30] Wildlife Protection Act, 1972, section 19.
[31] Wildlife Protection Act, 1972, Section 23.
[32] Forest Conservation Act, 1980.
[33] *Banbasi Sewa Ashram v. State of U.P.* 1987 SCR (1) 336.
[34] W.P. No. 202 of 1995.
[35] Madhu Sarin, 'Undoing Historical Injustice - Reclaiming Citizenship Rights And Democratic Forest Governance Through The Forest Rights Act', *Democratizing Forest Governance in India* (1st edn, Oxford University Press, India 2014).

managed traditionally for generations.[36] The objective of the FRA is to recognise and vest forest rights. It is a benevolent piece of legislation[37] and a remedial statute aimed at securing social welfare.[38] The pertinent task here is to ensure awareness amongst the tribal and other traditional forest dwellers of their rights and their ability to access such technology without hindrance.[39]

However, the over-reliance on satellite evidence as a form of evidence collection can hamper the process of vesting rights among other things mentioned in the FRA. It envisages a proactive role by the Gram Sabha to increase stakeholder participation. Yet, due to inaccessibility and lack of awareness, the Gram Sabha often relies upon inaccurate reports. The same reports are in turn used for future dispute settlement by the divisional and state authorities. The maps used are generic Google Earth images or low-resolution satellite images (old LANDSAT images) which are outdated. Rule 13[40] of Scheduled Tribes and Other Traditional Forest Dwellers (Recognition of Forest Rights) Rules, 2007 (the Rules) mentions the evidence for determination of forest rights wherein 13(1)(a)[41] counts satellite imagery as evidence. Section 12 A (11)[42] explicitly mentions that the use of satellite imagery should only supplement the evidence and not replace the physical form of gathering evidence. The over-reliance on maps as a piece of substantial evidence and not backing it up by technological advancement is also worrisome. Forest are dynamic in nature and shift and change in quick successions, therefore the reliance should be on extensive field mapping and should be supplemented by advance satellite imagery.

III. CRITICAL APPRAISAL OF ITS EVIDENTIARY VALUE

The application of Satellite data for forest conservation and wildlife protection differs from its usage in other environmental law concerns such as mining, industrial operations, pollution, or climate change analysis. Its successful integration with every other field of

[36] 'Undo Historical Injustice to Forest Dwellers, Once Again' Oxfam India https://www.oxfamindia.org/blog/undo-historical-injustice-forest-dwellers-once-again#:~:text=What%20is%20the%20Forest%20Rights,and%20managed%20traditionally%20for%20generations.

[37] The Scheduled Tribes and other Traditional Forest Dwellers (Recognition of Forest Rights) Act, 2006, Preamble.

[38] *Union of India v. Akhil Bhartiya Vikas Parishad* (2010) 12 SCC 375.

[39] *Orissa Mining Corporation v. Ministry of Environment and Forest*, WP (Civil) No 180 of 2011.

[40] Scheduled Tribes and Other Traditional Forest Dwellers (Recognition of Forest Rights) Rules, 2007, Rule 13.

[41] Scheduled Tribes and Other Traditional Forest Dwellers (Recognition of Forest Rights) Rules, 2007, Rule 13(1)(a)

[42] Scheduled Tribes and Other Traditional Forest Dwellers (Recognition of Forest Rights) Rules, 2007, Rule 12A (11).

environmental law has led critics of FRA and conservationists to ask why this thoroughly vetted technology is not enough for Forest Conservation. It is in biodiversity conservation and wildlife protection that satellite data meets its most cynical sceptic and ardent supporter.[43] Therefore, the jurisprudence evolved in this regard requires a distinct critical appraisal. Under the FRA, according to Rule 13 of the Rules, there should be at least two pieces of evidence used to advance a particular conclusion.[44] When approaching the higher courts through writs, the courts should give effect to this requirement under the FRA.

Three-Tier Quasi-Judicial System Under the FRA

As discussed earlier, the primary legislation where satellite imagery finds an explicit mention and utilisation is the FRA. Therefore, in this section, we will explore the nature and quantum of value attached to satellite imagery vis-a-vis cordoning off forest areas and settlement of forest rights under the FRA. It provides a framework for recognition of such vested rights and the nature of evidence required for such recognition and vesting. It follows a three-tier quasi-judicial system including the Gram Sabha, the Sub-Divisional Level Committee (SDLC), and the Divisional Level Committee (DLC). According to Section 6, the Gram Sabha is authorised to initiate the process of rights recognition of the individuals and communities.[45] It receives the claims, verifies them, passes a resolution recommending approval or dismissing the same. Any person or state agency aggrieved by the resolution of the Gram Sabha can petition before the SDLC within 60 days of passing of the resolution.[46] If they are unsatisfied with the decision of the SDLC they can further prefer a petition against it in front of the DLC.[47] The SDLC and DLC must give the aggrieved person a reasonable opportunity to present their case.[48]

[43] *Action Research In v State of Gujarat*, W.P. No. 100 of 2011, *Wildlife First Case v Ministry of Forest and Environment* W.P. No. 109 of 2008.
[44] Scheduled Tribes and Other Traditional Forest Dwellers (Recognition of Forest Rights) Rules, 2007.
[45] The Scheduled Tribes and other Traditional Forest Dwellers (Recognition of Forest Rights) Act, 2006, Section 6(1).
[46] The Scheduled Tribes and other Traditional Forest Dwellers (Recognition of Forest Rights) Act, 2006, Section 6(2).
[47] The Scheduled Tribes and other Traditional Forest Dwellers (Recognition of Forest Rights) Act, 2006, Section 6(4).
[48] The Scheduled Tribes and other Traditional Forest Dwellers (Recognition of Forest Rights) Act, 2006, Section 6(4).

Section 11[49] talks about the procedure for filing, determination and verification of claims by the Gram Sabha. Section 11 (2) further directs the Forests Right Committee to assist the Gram Sabha in collecting evidence by maps. Rules 13 (1) and (2) of the Rules provide a comprehensive list of evidence which can be used by the forest dwellers to prove and existing rights. Rule 13(1)(a) enlists satellite imagery as one such acceptable evidence. Rule 13 (3) further provides that the Gram Sabha, SDLC, and DLC must rely upon a minimum of two evidence.[50] Moreover, during the settlement of rights process and declaration of a Critical Wildlife Habitat under the FRA, Section 4(2)(b) stipulates that the concerned agencies must establish that the presence of the right holders is sufficient to cause irreversible damage and threaten the survival of the species and their habitat. Therefore, it indicates a high standard of proof wherein there must be a direct correlation between the activities of the forest dwellers and the reduction in forest cover. Reading together the provisions of the FRA and the Rules, the authorities must prove based on certain and objective criteria that the presence of the forest dwellers is detrimental to forest conservation and wildlife protection. Rule 12 B (11) (2) clarifies that a simple reliance on satellite data is not enough to fulfil this requirement and therefore, it must be supported by additional evidence.[51]

The jurisprudence of Forest Conservation and Forest Rights

Under writ jurisdiction, the High Courts and the Supreme Court do not participate in fact-finding, therefore do not engage with the general principles of evidence law.[52] However, satellite imagery is used as substantial evidence while accepting or rejecting a claim at the quasi-judicial level. Oftentimes, the interests of Forest Dwellers are pitched against the interest of Forest and Wildlife. This begs the important question of how to adequately balance these rights for which substantial evidence forms an integral part. Inaccurately determining the cause of deterioration of the Forest and the Wildlife harms both, the forest dwellers and the Environment. Therefore, in the interest of justice and social welfare, the courts must include a certain framework in its orders with regards to interpretation and usage of satellite data by the state bodies. Otherwise, there will be a huge lacuna and uncertainty

[49] The Scheduled Tribes and other Traditional Forest Dwellers (Recognition of Forest Rights) Act, 2006, Section 11.
[50] Scheduled Tribes and Other Traditional Forest Dwellers (Recognition of Forest Rights) Rules, 2007.
[51] Ibid.
[52] *K.L. Mysore v. State of Mysore*, 1976 SCR (3) 913.

regarding the usage of satellite data. Wherein, the ground realities do not match with what the legislation requires or what the Courts order.

Action Legal Research In. V State of Gujarat

The Gujarat HC observed in the case of *Action Research In v State of Gujarat,*[53] that satellite imagery on its own is a weak piece of evidence. In this case, the petitioners approached the high court citing that the State had made a highly unscientific use of satellite imagery while settling claims. They claimed had indulged in a defective, unsatisfactory, and illegal method. The petitioner also prayed that the use of satellite imagery should be transparent, along with the active involvement of the claimants and the Gram Sabha as envisaged by the FRA. They further prayed that satellite data be used as only one of the acceptable evidence along with other pieces listed in the Rules and that claims should not be rejected solely based on satellite data.

The Gujarat High Court in this case opined that the FRA being a benevolent piece of legislation requires special consideration. The Courts are dutybound to adopt a constructive approach to achieve the purpose of the FRA. To demand strict proof of rights from underprivileged and marginalized citizens would frustrate the very objective of the FRA. It also considered the fact that being illiterate and specially situated, such forest dwellers would lack any strong and convincing evidence which could satisfy the authorities. However, this does not mean that every claim should be accepted at its face value but rather that satellite imagery should not be the only evidence used to accept or dismiss a claim.

Therefore, owing to the uncertain nature of satellite data, they must always be supplemented with other strong pieces of evidence along with the practice of ground-truthing.[54] Ground truthing refers to the information collected on location and the ground. It aids in the interpretation and analysis of the data and helps minimise the errors of omission and errors of commission.[55] Hence, a singular reliance on satellite imagery is not enough. This position is akin to general international practices wherein satellite data must be supplemented with a thorough in-field observation and data collection.[56]

[53] WP (C) 100/2011.
[54] *Action Research In v State of Gujarat*, WP (C) 100/2011.
[55] J.B. Campbell, *Introduction to Remote Sensing*, The Guilford Press, New York (1996).
[56] Sharon Hatch Hodge, 'Satellite Data and Environmental Law: Technology Ripe for Litigation Application', PELR (1997).

Wildlife First v Ministry of Forest and Environment

In the ongoing case of *Wildlife First Case v Ministry of Forest and Environment,*[57] the Supreme Court is assessing the constitutional validity of the FRA. In February 2019, initially, the apex court had ordered the states to evict individuals with rejected claims by the concerned authorities. This would result in the eviction of as much as 10 lakh tribal people, the second wave of a mass eviction. However, after public outcry, it later placed a stay on its previous order and asked the Forest Survey of India (FSI) to conduct a satellite survey. The FSI is required to collate the data from various states and corroborate its findings. The FSI has informed the Court that it would take it 16 years to do so given the lack of adequate funds and need for cooperation from the various state machineries.[58]

There are numerous State-sanctioned studies and reports which testify to the increased accountability and transparency accompanied by reliance on satellite imagery.[59] State agencies have made extensive use of this technology by assigning several independent agencies such as the Saxena Committee appointed by the Ministry of Tribal Affairs, TERI appointed by the Maharashtra Government, and BISAG appointed by the Gujarat Government.[60] Wildlife First, an NGO and also a petitioner to the present case, believes that the reports clearly show a rapid encroachment of forest lands and that most of the claims are bogus.[61] The FSI initially filed an affidavit in the case to claim that "satellite imagery shows massive encroachment after the Forest Rights Act was enacted".[62] Firstly, the FSI is responsible for ascertaining the forest cover in India. It is not the authority to comment or determine whether or not the claims of the forest dwellers are legitimate. Secondly, such rhetoric without adequate data collection does not take into account whether such a reduction in the cover is caused by legitimate cultivation by people whose claims were accepted and settled. Or whether the reason is different altogether. Therefore, satellite imagery in and of

[57] WP (C) 109/2008.
[58] Ibid.
[59] Bhavya Goswami, 'Geo-informatics for Forest Rights: Harnessing Technology for Better Livelihood Support and Access to Forest Rights', One World Foundation India (2014)
[60] Meera Bhardwaj, 'Satellite Imageries, the Only way to Clear the Forest Rights Act Mess', Green Minute (2019) https://greenminute.in/2019/07/24/satellite-imageries-the-only-way-to-clear-the-forest-rights-act-mess/
[61] Shruti Agarwal, 'Can Technology Support Forest Rights Process?', Down to Earth (2017) https://www.downtoearth.org.in/blog/governance/can-technology-support-forest-rights-process--59345
[62] Satellite imagery shows massive encroachment after Forest Rights Act was enacted, Deccan Chronicle 2020 https://www.deccanchronicle.com/nation/in-other-news/200120/satellite-imagery-shows-massive-encroachment-after-forest-rights-act-w.html

itself does not provide us with the reason for the reduction of forest cover but only that there has been such a reduction.

The problem here is not the reliance on the Satellite imagery but an exclusive and uncritical reliance. Without ground-truthing it becomes impossible to deduce and verify how the land is being used thereby rendering the interpretation of encroachment incorrect.[63] The anti-FRA petitioners and the Supreme Court have placed heavy reliance on Satellite imagery to determine the validity of claims. But the Rules clearly provide that they can only supplement other forms of evidence, and cannot be used as a replacement.[64] Therefore, the use of technology should be accompanied by additional evidence in the interest of justice and science. The evidence provided by the Forest Department was inadequate in proving that the claims of the forest dwellers were bogus.[65] While satellite data undoubtedly has its benefits, it cannot make up for the intricate facts which are unearthed by local, on-site data collection and verification.[66]

IV. RECOMMENDATIONS

The problem with satellite imagery remains in its implementation and lopsided interpretation. So long as the technology requires considerable human coordination, it runs the risk of a biased application. Difficulty arises when the State tries to monopolise it and use it in a non-transparent manner, overlooking the inherent discrepancies in order to get the job done. It becomes even more problematic when the agencies claim that these are 100 percent accurate and objective.[67] Contesting the same is especially challenging for the underprivileged and marginalised communities. On the one hand, Satellite Images can be produced swiftly, are cheap, and labour free. On the other hand, they are often used unscientifically. When they are used properly they can take as much as 16 years to provide comprehensive data.[68] The critical question that arises is how to strike a balance between a

[63] Ibid.
[64] Scheduled Tribes and Other Traditional Forest Dwellers (Recognition of Forest Rights) Rules, 2007, Rule 12 A(11).
[65] 'Manthan: Report of the National Committee on Forest Rights Act', A Joint Committee of Ministry of Environment and Forests and Ministry of Tribal Affairs, Government of India. December 2010.
[66] Nandini Sundar, 'A Mahagatbandhan in the Forests is the Need of the Hour', The Hindu Centre for Politics and Public Policy, https://www.thehinducentre.com/the-arena/current-issues/article26978490.ece/binary/A%20Mahagatbandhan%20in%20the%20Forests%20is%20the%20Need%20of%20the%20Hour.pdf
[67] Shruti Agarwal, 'Can Technology Support Forest Rights Process?', Down to Earth (2017) https://www.downtoearth.org.in/blog/governance/can-technology-support-forest-rights-process--59345
[68] WP (C) 109/2008.

quick but sloppy work and a thorough but time-consuming approach. In the 16 years that it takes the agencies to come up with the data, the entire mapping process might become futile if the species and habitats become endangered.

Therefore, the key to resolving the conflict lies in a bottom-up approach towards implementation as also envisaged under the FRA. By increasing transparency and a true collaboration on the ground level, it will decrease the risk of a biased application. As the Hon'ble Supreme Court itself held in its landmark judgement, it is the village and the Gram Sabha which are primarily responsible for recognition of forest rights.[69] The Gram Sabha and the communities must be empowered and systematically included in the mapping process.

The Narmada district of Gujarat is the perfect example of one such beneficial collaboration. With the help of Action Research in Community Health (ARCH), an NGO, the Forest rights Committees from 150 villages learnt the use of GPS and GIS. They then mapped the claimed plots and superimposed them on satellite images from 2005 and 2009. First, to determine the status of the lands in 2005 and then on the image from 2009 to determine possession post the enactment of FRA.[70] Ensuring proper and error-free implementation at the ground-level will reduce the chances of error and conflict later on. Thereby, reducing the complexity and the time consumed in settling claims and conserving forest lands. After all, doing a job thoroughly once is more efficient than doing it poorly multiple times.

V. CONCLUSION

Technology is a part of every realm of our society in the contemporary era. It is often considered to be more precise and quick than manual work. The environment conservation regime has also introduced the use of technological tools in various aspects, satellite imagery being one of them. Agencies rely on Satellite imagery for identifying areas to conserve and protect. Although it is a labour-free and expeditious way of collecting evidence, it is not completely reliable. Owing to the misapplication of satellite data which often results in inaccurate conclusions, the Rules categorically provide that such data should not be used unaided. They further require the use of minimum two pieces of evidence. When such cases

[69] *Orissa Mining Corporation v. Ministry of Environment and Forest*, WP (Civil) No 180 of 2011.
[70] Action Research in Community Health and Development- Gujarat, 'The Forest Rights Act, Implementation of the FRA' https://archgujarat.org/the-forest-rights/

are raised in the Courts, the courts must give due regard to the rationale behind this prerequisite. In its current application, the concerned authorities often perform a shoddy job of data collection by relying on a questionable data set and incorrect interpretation.[71] There are three misapplications of satellite imagery in Conservation. Firstly, at the ground level, old data is used unscientifically without supplementing it with ground-truthing. While the use of generic Google Earth Images is wide-spread, it should be accompanied by data collection. Secondly, the images produced often lack reliability. The agencies that the State authorities engage in produce faulty data which is used uncritically. And thirdly, the judiciary has given its spin to the interpretation without taking into account the checks and balances put into place by the FRA. These three distinct approaches make its application ambiguous and leave a gaping hole in the implementation of the FRA. Since satellite imagery is a substantive piece of evidence, an incorrect premise will lead to incorrect conclusions. Therefore, if the conservationists and state agencies indeed wish to protect biodiversity, then they should push for the strengthening and proper bottom-up implementation of the FRA. Its dilution and misapplication by reducing the evidentiary requirement will be counterintuitive for conservatio

[71] Ibid.

TECHNOLOGICAL EFFECTS ON RIGHT TO PRIVACY WITH SPECIAL REFERANCE TO MEDIA TRIAL

Dr Santosh Sharma[1] and Sakshi Vashisth[2]

ABSTRACT

This is the indicator of the very statement to no-one is over by law while the creation of India definite autonomy of appearance and verbal statement to its people, society. it's the liability of judiciary to acknowledge along with provides make to liberty of media. The media are covering extensively crime situations or suspect of a specific crime alarmingly. it's ably aforesaid by Law Commission of Asian nation that there seems to be little restrain within the media in thus for because the Administration of Criminal Justice worries. The assessment by media could be a expression created in style in the last 20th century and early on 21st century. within new period around various instance during Through which media have conduct the examination of Associate in Nursing suspect and has announced the result yet prior to the Court pass its decision. several noted heinous cases that will have vanished unmanageable except by the involvement of Press, square measure Priyadarshini Matto matter ,Jessic case, Nitish Katara assassinate case and Bijal rape case. The fair rule of Indian statute, consisting of Articles14,19 and 21, Presume a huge significance in this esteem nowadays trial has shift from judges Courtroom to living area. and also corporation sells share to a media concern in trade for Promotions, break and positive exposure. There is a need for a self-regulatory as well as statutory authoritarian power with to control exposure of offensive matter, therefore it is suggested that rules and regulations must be framed in this regard. There is necessitate for comprehensive rule on coverage of *sub- judicial* cases. thus Right to Privacy law must be introduced and active structure of media rule is to be lawfully changed to comprise detailed rule main discovery of confidential in order by the media.

1.Indian medium :An advancement

Journalism in our democratic state glorious is understood is thought because the Fourth Estate that means thereby that it's as vital as different 3 identified organs of the status i.e. legislative assembly, government and therefore the law lords. Media could be

[1] Associate Professor, Dr. K.N Modi University, Newai Tonk
[2] Research Scholar, Dr. K.N Modi University, Newai Tonk

a support in favour of a self-governing setup, as from first to last the intermediate of group media concepts crossways society square measure communicate; these an assumption open place measure base of contribution and dialogue. concurrently, the independence of media have be acknowledged still since secluded by the Indian Supreme Court below Art. 19 (1) (a) that is correct to liberty of communication. Indian Press have approach back archaic, as of organism solely operate with the country to the company by United Nations agency square measure for the most part see because skilled with impartial in their reporting of the trial. resting on its beginning media be presented with bags of autonomy in order so as to balanced, methodical and truthful reportage might be completed all the cases .The highest court of Indian definite paper case created the subsequent explanation–"The idiom "freedom of the press" have not been utilize in editorial nineteen however is apprehended in Article 19(1) (a). fight and want to stay pertinent, information network take positive original initiative for the 'civic at large'. whereas popular of media movement square measure optimistic, function of Press in investigatory reporting of cases unfinished assessment is uncertain. within the Old Delhi mob rape case wide referred to as 'Nirbhaya case' the media has obsessed the position of associate degree campaigner however have reportable matter of sexually evil doing inconsiderately and while not owing to attentiveness. The new NUJS regulation imprison matter and "Tehalaka" case square measure different instance within by which the Press has became personality announce impartiality structure by classification and creating uncorroborated allegation. one in every of the article 'trial and error' have terribly exactly elaborate this: -

1.1 communal Rights Vs. personal Rights

Liberty of journalists have been expound by highest Court during sequence of decision. In Romesh Thapar v. State of Madras5 it had been command that the liberty includes the liberty of concepts, their journal as well as distribution. Media in cases like Jessica lal matter and Priyadarshini matto case have bring integrity that has been elusion the dead fatalities for duration. Media's movement pass balance in matter relating made and prestigious suspect, wherever probability of 'fair trial' while not vigilance don't exist. Like, in Jessica Lal case, suspect Manu Sharma son of Vinod Sharma INC Minister from Haryana was clean-handed by the judicature primarily because of 'police failure to ascertain an entire series of the conditions resulting in the happening' ands 'all 3 eyewitness scheduled by the police force within the written account become antagonistic throughout the trial' highest Court

of Asian nation have occupied memo of complaint for intensive reporting and conversation on sub-judicial cases in electronic still as medium. just in Sahara case, the supreme court in a very call by Honourable S H Kapadia make instruction for rescheduling charge as matter intolerance is cause by Trial information. emphasize objective of such a tenet was to stop attainable disdain command below Article 129 or 215 of the statute of Constitution against the Journalism for his or her detrimental reports.

2. lawful implication OF Journalist's 'activist responsibility

The investigatory the information of journalist lead to inflicting additional damage than profit in examination of heinous offence. The results of the Media trials on call in court is established is some ways, such as.

2.1 psychological ordeal –

The information of journalists transferral crime of sexual temperament focused of the final community to dialogue. to administer a look to the story, tortuous details square measure other within the report, that disclose the personality of the sufferer although real name isn't unconcealed. ' when Anti-Rape regulation, position has modified during this matter by amendment in Criminal Procedural Act 1974 and proof Act. it should be attainable, that sufferer might not be eager to debate or see the small print of the happening once more because of physical still as mental trauma. because of dialogue by public at giant, she could ne'er be ready to march on in her life.

2.2 Verbatim re-production -

The victim must agree and think about the first proclamation as any regular change as of the primary accurately statement that is accessible within the property right can fail the closing case of the tribunal at trial These open statement created by sufferers/witness is used throughout the trial, if there square measure contradiction. therefore, the public prosecutor would possibly find yourself lose critical evidence of one of its important testimony.[3]

[3] objectives of Press Council Act, 1978. An Act to establish a Press Council for the purpose of preserving the freedom of the Press
and of maintaining and improving the standards of newspapers and news agencies in India.

2.3 Knowledge and adherence of Criminal Manuel-

Today journalists square measure unwittingly commits violate of regulation of law and precise legislative lawful necessities. For, benevolent face to a tale and sensitive detailed tortuous of the incident is unconcealed. In option of that Sec. 228A of the Indian Penal code 1860 is exclusively been broken.

3. HUMAN RIGHT AND TRIAL BY MEDIA-

It can be noticeably match by the immediate of take into custody, looking the conditions of the matter. truthful assessment guarantee should be discovered as of the instant the enquiry beside the suspect commence till the legal trial, as well as some attractiveness, are concluded. [4]the excellence between pre- trial procedures, the particular trial and post trial procedures is usually unclear indeed, and also the infringement of civil rights throughout single phase can have an contact on other phase.[5]

3.1 PRE-TRIALS HUMAN RIGHTS

- The prevention on logical detain and custody
- . The Right to be acquainted with the reason for detain
- The Right to lawful guidance
- . The Right to a without delay advent before a megistrate to confront the legality of detain and custody
- The prevention of torment and the Right to humanitarian s Basic ituation through Pre-trial custody
- The prevention on Incommunicable do custody

3.2 THE HEARING

- equivalent right to use to, and justice prior to, the Courts
- The Right to a communal trial
- The Right to a expert, sovereign and neutral Tribunal recognized by Law
- The prevention on Self- incrimination
- The Right to protect himself in human being or in the course of lawful support

[4] Manfred Nowak, U.N. Covenent on Civil and Political Rights, CCPR Commentary (N.P. Engel, Arlington: 1993)
[5] Lawyers Committee for Human Rights, What is trial, Basic Guide to Legal Standard and Practice, March 2000 Originally prepared by Jelena Pegic in 1995.

3.3 POST-TRIAL RIGHT

- The Right to plead
- The Right to recompense for Injustice

4. ROLE MEDIA TRIAL'S IN INDIA-

The effect of television and paper reporting on U.S.A. are tremendous, little distrust or therefore no logic is being agreed. so, trial undertaken almost by these kinds of journalism even have turn into terribly effectual and most important in India, ever since the last era. we have a tendency to area unit aware that it absolutely was only because of a number of the journalist personnel's commitment that arouse society conflict within the sort of demonstration and objection march so as to be capable to set up justice within the Jessica Lal murder case. Even the any delay within the final finding of fact of Kasab was hindered because of the varied discussions, polls and reactions of individuals that were being transmitted to the govt officers directly or circuitously through the media. UN agencyle|the complete} nation became pissed off after they examine the figures of cash that were being spent to supply 'security' to an individual who unmercifully shot and killed innocent folks. in contrast to several alternative rape cases that are unfinished within the courts for years, the law enforcement agency, ministries and judiciary were driven to provide special importance to the present case [Nirbhaya Rape case, because it is usually best-known as] thanks to the large upsurge of the general public.

4.1 Trial by Media-

The Apex Court have above so as to the elemental rights to confidentiality and a good trial emanate of the broad right to living contain in editorial twenty one of the Constitution. In Kharak Singh v. State of Uttar Pradesh[6], the Supreme Court supposed that the correct to confidentiality was Associate in Nursing "necessary element of non-public freedom "which is "a right to be liberated from limitations or contravention.

In Zahira Habibullah Sheikh v. State of Gujarat[7], the Apex Court explain that a "fair trial clearly would denote a shot by Associate in Nursing fair choose, a good functionary and

[6] 1963 AIR 1295, 1964 SCR (1) 332

[7] CASE NO.: Appeal (crl.) 446-449 of 2004

ambience of court composed. honest trial suggests that a shot within which prejudice for or in opposition to the suspect, the witness, or the reason that is being try is eliminate.
though, sensationalized reports spread by the journalist have steady gnawed at the guarantee of a right to a good trial and display a severe risk to the assumption of virtue.

Why Unethical ?

It would be associate degree unethical apply with to hold away such practical trials by the journalist as a result of the judge's quality are going to be at pledge. will we watch for the 'fair' lawful trial to be over before remark after that The country does not enable USA to open or comment on a finding of fact. remark or comment unconstructively on a decision may finally end up in disrespect of court.

To Ponder Upon

Why was the rape case of Nirbhaya[8] given a special standing by courts of law? Why were even the ministries agitated to the extent, that, new laws were developed, new departments of police were opened to cater women's want, new helpline numbers were opened womans} safety? the explanation is that the media's constant coverage of the incident elevated it to a high-profile act wherever the girl was a created a 'symbol' of all the oppression that girls face within the country. Journalists had in no manner taken to unethical observe so as to earn 'brownie points' within the sort of TRP.

4.2 Information expertise in Courts

It a element of the learning to begin by a debate of knowledge skill in courts. previous to explore judicial improvement, it's helpful to possess a way of what we all know regarding IT in bench. it'll inspect the various functioning of courts use. The query to reply is what IT functioning are enforced within the courts, and for what functions area unit they used.

4.3 Court IT's

In an early on illustration of the utilization of data knowledge within the court, the conflict crime tribunal once war second created utilize of pictures objects and coincidental transformation. Today, many various sorts of IT area unit employed by the global organization International Criminal Courts and and video recording of the court session,

[8] SCC, 2012

coincidental explanation, electronic court reporting, videoconferencing for observer hearing, and electronic records. furthermore, the court preserve internet site with their selection, surroundings data, and sound and pictures as of the court.

4. Judicial Technology's

In ordinary law judiciary system, in each communal and illicit integrity, matters are eventually set beside trial if they're not developed in Associate in Nursing former section. only a only some cases truly return to trial, and trial rate vary wide crosswise country. a number of those trials are conduct before of a judges. In those trials, the code of propinquity of proof is incredibly vital. this implies the proof oneself must be conferred within the tribunal witness creating an announcement, exhibit similar to new papers and objects. This has give increase to performance of knowledge technology to hold up conduct trials. proof cameras are wont to gift exhibits like documents, pictures or objects. otherwise of present such exhibit is thru their picture on a personal computer pc associated to the show instrumentation. monitor and digital projectors and screen are wont to show the exhibit. The kill switch may be a tool for the choose to manage what jurrist authorized to determine in accord with testimony system

5. Law Commission Report-

The most calculated and complete study on the optimistic and unconstructive sides of trial journalists have been explained in two hundredth report of the Law Commission titled "Trial by Media: Free Speech vs. honest Trial underneath Criminal Procedure (Amendments to the Contempt of Court Act, 1971)". This report was submit on thirty one.08.2006. numerous amendments are urged to deal with the harmful effects of exaggerated and dramatized information reports of news paper, and victimization of the suspect/accuse by media, on the management of justice. The Law Commission has counselled to ban publication of regardless of what's prejudicious to the defendant and a constraint that shall perform by the moment of take into custody. it's additionally advocated that the judicature be unconditional with the facility to through adjournment of journal or broadcast in immoral cases. The commission has any ED so as to at the present, such publications square measure contempt as long as a rap sheet had been LED in a very criminal case.37 once citing numerous case laws and authorities on the subject38, the Commission has projected that the start line of a criminal case ought to be from the time of arrest of associate degree defendant and not from the time of ling of the rap sheet. within the legal instrument of the Commission

the projected change would keep a check on the media. The Law Commission has any urged that the judicature ought to be authorised to delay publication or broadcast about a criminal case by the print and electronic media and to control the media from resorting to such journal or telecast. In Chapter IX, the Law Commission has specie ED numerous codes of conduct by the media and journalists to curb the menace of interference within the direction of justice. The Law commssion has additionally counselled that journalists ought to be trained in sure aspects of law about freedom of speech in Article 19(1) (a)[9] and also the limitations that square measure allowable underneath Article 19(2) of the Constitution, individual rights, law of denigration and contempt. it's any urged that these subjects be enclosed within the program for journalism and particular sheepskin or amount choice on newspaper journalism and law be going ahead.

6. Conclusion & Suggestion:-

There is a broad read with the purpose of the difference among associate defendant and a offender and the fundamental original standard of 'not guilty till established guilty' area unit frequently unnoted by devision of the journalism in its reporting of in progress trials. By conduct similar trial, the media, it is feel, not solely put excessive load on the decide however conjointly create load on lawyer to not get up cases of defendant.

Now a days trial has shift as of room to lounge. and therefore the results of such a move is that rights of individuals rise to be affect in a very mode so as to has not see ever before. Media these days is commercial and globalised. single cannot envision communal liability on the up to date commercial media. Their main aim is revenue. though, as all come for a value in today's present time, the earnings creating too has some value. and therefore the price is individual rights of the defendant. The role compete by media has crystal rectifier to the persecution of not guilty individuals and infringement of their basic civil rights. The defendant is command culpable yet by the start of the path. as an example, the recent controversy arise once the Jamia Encounter has raised several queries relating to the responsibility of the media in such cases. Such devil-may-care manner of functioning could be a obvious infringement of the moral values that type the substratum of a civil society. "The media conjointly creates different issues for witness. If the personality of witnesses is revealed, there's risk of the witnesses returning besieged each from the defendant or his acquaintances moreover as from the police. Being an area of the civil society media

[9] P.M. Bakshi, The Constitution of India Page no 48, Universal law publishing, thirteenth Edition.

incorporates a helpful role to play to examine that their devil-may-care manner of functioning doesn't lead to the violation of the rights of the individuals, that area unit compactly brought up as ‘Human Rights’. finally, one among the abundant debate problems has been the power of the media on the option creating process of the judges. Consciousness reporting has conjoin on the judiciary.

SUSTAINABILITY THROUGH GREEN-BUILDINGS: A STUDY WITH RESPECT TO REAL ESTATE, ENVIRONMENTAL PROTECTION, AND THE SDG'S

Stella Joice[1]

Abstract

The fast growing pace of the development has caused a vast devastation to the environment all over the world. The agricultural lands are covered up with the skyscrapers building. The fast growing financing availability through the financing agencies and the growth in the income of the people has created a much higher demand for a higher standard of living. The demand for the infrastructure known as the eco- buildings or the green building have nowadays increased with the need that has arisen for the contribution towards maintaining of the environmental balance and the sustainable development. The devastating elements whether natural or man-made has caused the various imbalances to the environment causing the increase in the pollution, disturbed weather conditions, uneven water level, the depletion of the Ozone Layer, the decrease in the number of the species of the plants & animals, the increase in the humidity, global-warming and the climate change. The levels of concerns have been showed by the National and the International Agencies towards adopting green technologies to conserve and preserve the environmental. The UN celebrating its 75th Anniversary and the 5th Anniversary of the Sustainable Development Goals sets us a target that the need towards the adoption of the eco-friendly regime needs to be implemented more in our lives. The Real Estate world is no exception to this. The practice of adopting the green building projects by the real estate owners and the infrastructural designers will create a positive image adding to the cause to sustain the ecology with recycled materials and green layouts. The fulfilment of the sustainable development Goals towards eco-friendly living and earning will lead to the upliftment of the environmental balance to some extent. The protection of the environment forms an integral part of our ecology being a part of the contributory towards the sustainable development.

Introduction:

With the advent of science and technology in the Era of Globalization, the sustainable development of the human race has become a major concern at the National and at the International level. The environmental degradation has led to the process of upgrading the

[1] Academic Associate, School of Business & Law, Navrachana University, Vadodara

environment by way of introducing the technology to sustain the very existence of the human kind by experiment in the green technology. The buildings which has formed the crust of one's living and sustenance is exposed to the Millennium Development Goals to maintain the eco-friendly buildings for the growth and healthy living. The modernised concept of the Green buildings has grown with the times to achieve the goal to abide in the very shelter of green homes and green offices.

Constitutional protection to Environment:

The Fundamental Rights and the Fundamental Duties enshrined in the Constitution guarantees the Environmental Protection so as to maintain the sustainable development goals. The Article 14 provides for the State shall not deny to any person the equality before the law or equal protection of the laws within the territory of India. This article 14 of the Part III plays a very important role in the protection to the environment as it checks the arbitrariness of the various discretionary actions of the State Authorities and also gives the prominence to the principles of the natural justice, fair play and reasonableness. The second article which focuses on the eco-friendly justice is the article 21 which provides for the Right to protection of Life and Personal Liberty. The Judicial Activism has widened the scope of Article 21 and has been extended to the eradication of the environmental imbalance thus protecting the environment and providing the right to environment which is pollution free and healthy environment. The Fundamental Duty in the Article 51A(g) which provides for the duty to protect and improve the environment which covers the improvised sustenance through the green-buildings and the leading a life to a healthy environment.[2] The guaranteed support and the various remedies available in the Article 32 of the Constitution for the fulfilment of the Sustainable Development Goals has led to more of the infrastructure towards becoming green and eco-friendly.

Sustainability through Green-Buildings

A green or a sustainable building is that because of its construction and features, can improve or maintain the quality of the life of the environment in which it is located. Green Buildings are beyond the concept of the traditional construction and the includes the site planning, community and as well as the land –planning.[3] The applicability of the green buildings uses the minimum energy resources like solar energy and wind energy which in turn lessens the

[2] .Dr.N.Maheshwara Swamy: Textbook on Environmental Law(Asia Law House, 2nd Ed, Reprint 2020)
[3]Green Built Alliance,'Importance of Green Building'< https://www.greenbuilt.org/about/importance-of-green-building/>accessed 29 June 2021

cost of the productivity, the improved health of the human being, reducing the over impacts of the environmental imbalances.[4] According to T.H.Chan School of Public Health, people in green ,well – ventilated offices record a 101 per cent increase in cognitive brain function.[5]

The Indian Green Building Council (IGBC), Part of the Confederation of Indian industry (CII) was formed in the year 2001 so as to enable a sustainable built environment for all and facilitate India to be one of the global leaders in the sustainable environment by 2025.[6] According to the U.S.General Service Administration(GSA),mostly the green buildings consume 26% lesser energy and release 33% fewer carbon dioxide emissions. The Green and the sustainable practises try to reuse the existing buildings, recycled materials and local materials and propose the on-site recycling by using the less of the constructional material.

Green Buildings which has replaced the existing traditional infrastructure and its Construction in the real estate is not the same as the sustainable design, but it is the part of the sustainable design, which is related to designing and developing for the period of long term, with the advancements of the development adhering to the present needs without compromising the ability of the future generations to meet their own needs.[7] They improve the health and the thermal comfort of occupants by the improved indoor environment inclusive of the air quality, views, daylighting, comfort controls ,natural ventilation, and a connection to the natural environment. The various studies have revealed that the improvised quality in the air quality, natural ventilation, views, daylighting, comfort controls, and a connection to the natural environment has improved the productivity in their studies scoring them good and also that the indoor quality increased the increase in the number of the sales and the work productivity of the workers and earning good profit to the company or the firm.

The Manassas park Elementary School in Virginia is a sustainable project designed to meet the 2030 challenge and uses 50% less energy than a code-compliant school. This is an award winning green project which comprises of the spray-foam insulated which envelopes significantly surpasses the most stringent codes for the airtightness and insulation, while ground-

[4] Wienerberger,'Going green with Buildings-Building green is not a choice but a commitment for future generations '<https://www.wienerberger.in/green-building/why.html>accessed 29 June 2021
[5] P K Misra,'The Importance of Green Buildings in contemporary India'BW Smartcities Sophos (India,3 July 2020)
[6]BruntlandCommission1987:1 https://www.are.admin.ch/are/en/home/media/publications/sustainable-development/brundtland-report.html accessed on 1 July ,2021
[7] Indian Green Building Council,< https://igbc.in/igbc/>accessed on 1st June 2021

sourced heat pumps provide for the conditioned air to the classrooms only when it is needed. The windows are openable with green light mode indicators allows the students to know about the correct time to open the windows for natural ventilation throughout the classroom and when the indicator turns red the students have to close the windows. The sloped classroom ceilings and the light lowers funnel allows the daylight deep within the classes. The sensitise the students to the usability of the water and learn the importance of it the rain-harvesting is done on every roof and thus this harvested water is used for the toilet flushes and irrigational activities.

Thus this project related to the green building saves about 1.3 gallons of water each year. This Sustainable construction with the involvement of the green technology taking into account the three pillars of sustainability: the right of all people to live in a socially, economically, and environment friendly healthy building or community.[8]

In India the Real Estates sector is flourishing at greater pace with the speed of 112.2% Compound Annual Growth Rate (CAGR) Which leads to the increasing demand in the preservation and the conservation of the natural resources within the bounty of the nature Earth. By the end of the fiscal year 2030, India is expected to have GDP of 4 Trillion and Population of 1.5 billion.[9] The depleting resources from the earth, forces the human minds to think of the sustainable development so as to fulfil the demand and the supply of the resources to the future generations.

The Green Building Revolution started in India in the year 2001.It was a movement brought in with the establishment of the Indian Green Building Council by Conference of Indian Industries(CII) in cooperation with USGBC AND Green Building Council of the world. India saw the First rise of the Building in Green, The Sohrabji Godrej Green Business Centre, Hyderabad. With 7.50 billion Sq.ft of Green Buildings ,India tops the Green Technology and the Green Real Estate Industry. India has presently achieved more than 75% of the green dream and likely to lay the footprint of 10 million by 2022, said by V Suresh, Chairman of The Indian Green Building Council. Further statements were that India can be leader in Sustainable Built-environment with the support, guidance and the active involvement of the various stakeholders at the National and the International Level. The Rating systems of the Indian Green Building

[8] Thaghat & Dod,'The Inception and Evolution of EIA and Environmental Clearance process-Laying Emphasis on Sustainable Development and Construction'(2015)IJERA< https://www.ijera.com/papers/Vol5_issue3/Part%20-%202/E53022228.pdf> accessed on 2 July 2021

[9] V Rishi Kumar, 'With 7.50 billion sq ft of green buildings, India among the top 5 globally' The Hindu Business Line (Hyderabad,6 August 2020)

Council(IGBC) are designed in such a manner so as to meet the national Priorities fulfilling the Sustainable Development Goals laid by the UN.[10]

There are more than 5,975 green projects with 7.55 billion sq. ft with the green building and to be built considering the Green technology following the green-built environment of the Real Estate world. These governmental and the private projects have adopted IGBC's rating system Green Homes, Green Healthcare Facilities, Green Schools, Green Factory Buildings, Green Campus, Green New Buildings, Green Townships, Green Cities, Green, etc.[11] The World Green Building council has appreciated the efforts put in by Indian Green Building Council(IGBC) and also the 26 holistic ratings of design laid by it.[11]The UN Sustainable Goals are taken into account while the framing of the holistic ratings. India is a Signatory to the World Green Building Council and is recognised by various forums. According to estimates out of the registered projects across the world there are 37% are registered in India under LEED NC-USA.[12]

The Policy Initiatives for the Green Initiatives in India are Energy Conservation Act in the year 2000, Establishment of the Indian Green Building Council in 2001, Bureau of Energy Efficiency under ECA 2001 formed in the year 2002, Bureau of the Indian Standards published the National Building Code in 2005, in 2006 there was the Issuance of Energy policy draft and the Ministry of Environment and Forests makes Environment Impact Assessment necessary for all buildings with built area of 20,000 sq kms.,in the year 2007 the Green rating for integrated habitat assessment was adopted as the national rating system for green buildings in India, National Action Plan on Climate Change was launched in 2008 as well as the Integrated Energy Policy 2008 approved by the cabinet, Announcement of Smart Cities Program in India in 2014, India signed the first Union Climate Change Paris Agreement in 2015, the year 2016 witnessed the announcement for the first 20 Smart Cities in India and also that the State of Telangana and Andhra Pradesh adopted mandatory compliance measures for building efficiency.[13]

Due to the absence of the unstructured post construction performance, Green certified residential projects are yet to gain prominence. In the absence of a structured performance metric system buyers are less interested to purchasing of the premium residential plots. So the

[10] Ibid
[11] Ibid
[12] Prithviraj Dilip Mane, 'Green Buildings and Sustainable Construction'(2017)362
[13] Ibid 363

government is providing additional FSI to developers for encouraging their involvement in green projects. The Hospitality Industry in India are experimenting themselves with the environmental sustainability practices so as to promote corporate social responsibility and reducing operating costs.[14]

The Real Estate Regulation 2016 is silent on the topic of environmental sustainability. It mandates the builders to obtain a host of clearances before launch of projects is unresponsive to the environmental norms and the concept of sustainability. The RERA also does not lay down any stringent penalties on the builders who delay with the paper work related to environment. In some states the real estate developers have to get the clearance for the coastal regulatory zones while in some others have to provide the proper certificate in case located near to forest or near a bird sanctuary.

According to Dr. Prem C Jain, the RERA is silent on anything to do with the concerns of the environment. Further he says that it is the responsibility of the State to look into matters concerning the green building and that there should be proper implementation of the rules. The State Authorities should implement the rules and can work with the municipalities towards the attainment of the goal relating to the environment sustainability .[15]

The Pandemic has shown an increase in the appeals for more eco-friendly residual plots as well workplaces. Post-Covid the individuals have become more health conscious, well-being, comfort, etc. The demand of well-ventilated rooms and office –spaces, fresh water and ample daylight has increased with the minds towards the sustenance of one's life. According to WHO respiratory and lung diseases are the prime most top causes of death in the world over. The evolution of the green technology used to make the green homes and offices have optimised the natural light in the green constructional design and limit the usage of the artificial light.[16]

The Green Construction in India Lacks technical expertise to execute projects and the funding to pay for the construction. Another critical point herein is the role in catalysing India's Green Economic Recovery. Post-Covid there has been the drastic reverse in the flow of the economy in the market and thus the demand for the real estate has decreasing because of the less opportunity to invest in the residential or the office plots and the spaces. A number of

[14] Ibid
[15] 'RERA Silent on Environmental norms; no solution to delayed clearances' Money Control (India,5 June 2017)
[16] Medha Ahuja ,'The case for green buildings in India'(Observer Research Foundation,27 Nov 2020)< https://www.orfonline.org/expert-speak/case-green-buildings-india/>accessed 3 July 2021

Government schemes like the Pradhan Mantri Awas Yojana (PMAY) has been demanded for the multiple benefits and the various employment opportunities abiding it. The Eco-Niwas and the PMAY can jointly create a blend of green housing in the nation.[17] The Green Rating for Integrated Habitat Assessment(GRIHA) in another such initiative towards the green technological construction in India .[18] The government has mandated all the Central Government and the PSU buildings to attain minimum three stars rating. At the State levels in India the Government has promised to increase the size of floor-to-area ratio under the GRIHA initiative and to broaden the space for greener lawns and infrastructures inviting more of the income facilities.

According to the USGBC report States like Maharashtra, Tamil Nadu and Andhra Pradesh have been able to contribute towards greener buildings because of such initiatives.[19] As we are well aware that LEED is the world's leading green building project and performance management system, delivering a comprehensive framework in the view of green designs, operations and construction and also performance. It focuses on the all the basic amenities which is included under one roof like comfort, air quality and human health features.[20] Indian States with the various Initiatives of the states are trying to build up their standards to the LEED system with the available resources whether it be the materials, plot and the funding from the organisations. The Funding is a very important component as it is requiring a long-term investment in the newer concept of the environmental sustainability which form the green buildings.

In the report of the Green Growth and Sustainable Development in India, Towards the 2030 Development Agenda, Summary for the Policy makers: India's Eight- point Intended Nationally Determined Contribution aims at the social, economic, political development with the environment sustainability with the vision towards the fulfilment of the eight points as mentioned in the report. This report was laid out by the Ministry of Environment, Forest and

[17] Ibid
[18] Green Rating for Integrated Habitat Assessment(GRIHA)2019
[19] Medha Ahuja ,'The case for green buildings in India'(Observer Research Foundation,27 Nov 2020)< https://www.orfonline.org/expert-speak/case-green-buildings-india/> accessed 3 July 2021
[20] LEED,'LEEDv4.1'https://www.usgbc.org/leed/v41?creative=340431663522&keyword=usgbc&matchtype=b&network=g&device=c&gclid=Cj0KCQjw24qHBhCnARIsAPbdtlJpFRmni3q_5Z-ul1Ui

Climate Change recognising poverty eradication along with the green growth as India's Sustainable development narrative.[21]

Conclusion:

The Concern for the fulfilment of the SDG's laid down by UN, the real estate and the Green Technology is serving the government with the along with the various stakeholders at the national and the State level. The Government schemes for greener buildings are coming up with the economic boost to the real estate and contribute to environment –friendly green buildings and environmental sustainability. Even though the Real Estate Regulation has not contributed much to the greener revolution but the other sustainable steps of the Government have come up to balance the environmental needs towards a sustainable living. The constant and the timely implementation of Government Schemes and the policy makers will lead to the final achievement of the Sustainable Goals 2030.

[21] The Energy and Resources Institute,New Delhi, Green Growth and sustainable Development in India, Towards the 2030 Development Agenda, Summary for the Policy makers: India's Eight- point Intended Nationally Determined Contribution ,Points 1-8

E-WASTE A CATASTROPHE LURKING AROUND THE CORNER: INSIGHTS INTO ITS IMPACT ON THE ENVIRONMENT AND PREVAILING LEGAL REGIMES IN INDIA.

Agna Prem[1], Anakha Krishna[2]

ABSTRACT

During the past few decades due to the advancements in the field of technology and the adoption of revolutionary methodologies, there was a radical change in the usage of electronic, electrical gadgets. The fast-paced developmental activities, industrial revolutions, consumerism, urbanization, etc paved their way in escalating the overuse of such pieces of equipment. Gradually it accelerated the production thereby causing huge chaos in discarding electronic wastes without adopting proper management strategies. Haphazardly disposing of e-waste is a major gateway in causing a wide range of environmental pollution and related natural degradation. Recklessly throwing away such materials into nature caused degradation of the composition of the soil, water, and air. Apart from the presence of a high level of chemical contents in it, they also emit carcinogenic fumes while burning. A developing country like India faces a huge problem dealing with all the electronic waste which are manufactured in one's own country along with those which are illegally dumped by highly developed nations. It has become highly crucial to deal with this menace by adopting proper legal regimes that will have a greater impact on society. There has been a wide variety of conferences and conventions mainly aiming at this matter. In India, legal regimes including The Environment Protection Act, 1986, the Electronic Waste (handling and disposal) Rules, 2011, the Hazardous Waste (Management, Handling and Transboundary Movement) Rules 2008, The E-waste (Management) Rules, 2016, etc. play a very predominant role. In spite of the prevailing penal provisions, many such deteriorating acts still loom large. This paper aims to examine the impact of discarded electronic wastes on the environment, their management strategies, and the impact of legislation that regulates this menace, and their existing loopholes in the regimes.

[1] 7th Semester, BCOM LL.B (Hons) student, at School of legal studies, CUSAT, Kerala.
[2] 7th semester, BBA LLB (Hons) studentat School of Legal Studies, CUSAT, Kerala

INTRODUCTION

Over the past few decades, there has been an exponential growth in the field of technological advancements coupled with developments of electronic and electrical devices. A gradual transition from the agrarian era to the age of technology propounded the need to introduce shortcuts into our daily life. Technology is being introduced to every single aspect of our life. The enhancement of the Information Technology sector was a major reason which caused the higher generation of e-waste around the globe. The major cause for the piling up of e-waste is the adoption of "Planned Obsolescence" by the companies which tends to limit the useful life of the product purposefully[3]. The concerns regarding their disposal which are intertwined with ecological issues have urged governmental authorities all over the world to implement legal regimes and agreements to curb the menace. Electronic gadgets are replaced after a short span of time due to numerous reasons like the eagerness of consumers to purchase the advanced and latest upgraded edition of the products.

WHAT CONSTITUTES E-WASTE

E-Waste can be defined as the –"waste that is created when an electronic product is discarded after the end of its useful life". These complex mixtures of materials are also described as the 'Digital Rubbish', they are the fastest-growing source of toxic waste in the whole world. . Some of the common examples of e-waste are cell phones, computers, mainframes, monitors, compact discs, printers, scanners, fax machines, battery cells, TVs, medical apparatus, washing machines, refrigerators, Compact Fluorescent Lamp, air conditioners, etc[4]. These expensive products which have once fulfilled our wants and needs are discarded soon after it becomes unfit for use or to replace the same with an upgraded model. Only a very small portion of the entire generated wastes is recycled as the rest of them is dumped into landfills or even shipped to a developing nation. The threat produced from e-waste may be caused by direct contact with harmful metals, inhalation of the fumes from burning, or from the leaching of the toxic materials. They comprise materials such as plastics, ferocious and non-ferocious metals, and other substances like mercury, lead, cadmium, chromium, copper polychlorinated biphenyl, etc. which

[3] Sushanth Sareen, Future Shock: India might go the way of planned obsolescence, newslaundry, 31st Aug 2017, available at https://www.newslaundry.com/2017/08/31/technology-education-skill-development-and-entrepreneurship

[4] Available at https://www.step-initiative.org/e-waste-challenge.html

react with the surrounding to form other dangerous compounds. Various studies reveal that the huge accumulation of lead from the e-waste if released into the environment and comes in contact with the food we consume can cause severe damage to the kidney as well as the central and peripheral nervous system. There also prevail unsophisticated methodologies in extracting the gold, silver, and copper from electronic devices which tends to cause higher risk to all living creatures and the natural ecosystem.

Electronic products contain many hazardous and toxic materials causing environmental disparities. Television and computer monitors use cathode ray tubes(CRT's) having a significant amount of Lead in them. These toxic materials cannot be degraded or dismantled properly without expert advice and caution. It has the power to contaminate the soil, groundwater, and even the air. The sources of e-waste can be categorized based on different perspectives which include:

- Individual household and small business
- Large MNCs, Institution, Governmental house and Foreign Embassies
- Manufacturers and retailers
- E-waste from import
- Secondary market of old PCs

Individual household wastes are not a major contributor to waste, but an estimation of the exact quantity is difficult. This constitutes about 22% of the total computers in India. The rest of the 78% of waste comes from the business sectors including government departments, public or private sector, MNCs, etc. being the major contributors of e-waste the estimated waste dumped will be around 1.38 million. E-waste produced by manufacturers and retailers comprises around 1050 tonnes per year[5]. This includes defective IC chips, motherboards, cathode ray tubes (CRT's) produced during the execution process. Huge quantities of e-waste have been exported to countries like China, India, Ghana, and Nigeria which include monitors, printers, keyboards, CPUs, mobile phones, PVC wires, etc. Also, there are e-wastes produced from the secondary markets together with the production of TV, computers, mobiles, electric boards, etc.

A PEEK INTO SOME STUDIES AND REPORTS

[5] Available at https://www.assocham.org/newsdetail.php?id=6468

The Global E-Waste Monitor report of 2020[6] found that the world dumped 53.6 million tonnes of e-waste last year, among which only 17.4 percent was recycled. So the question that arises here is where does the remaining e-waste which has not recycled go? India stands in the third position after China and the United States with 3.2 million tonnes of e-waste. The report was concluded by stating that "The way in which we produce, consume and dispose of e-waste is unsustainable".

The drastic increase in the amount of un-recycled electronic waste dumping to the environment without proper scientific treatment is a major cause for the degradation of natural resources and the ecosystem as a whole.

According to the studies conducted by The Associated Chamber of Commerce and Industry of India (ASSOCHAM) "In India, Maharashtra contributes the largest e-waste of 19.8% but recycles only about 47,810 tonnes per annum and among the device, computer equipment contribute around 70% of the total e-waste in our country". Various studies reveal that e-waste that is generated from the computer and its related parts contributes to around 70 percent of the total e-waste in our country; it acts as a principal e-waste generator. Among the major metropolitan cities in India, Mumbai, Bangalore tops the list that contributes to an estimated 12, 20,000 tonnes of e-waste annually.

E-WASTE AS A GLOBAL CATASTROPHE

E-waste encompasses a variety of inputs and is considered the fastest-growing stream of hazardous waste in India. Based on both developed and less-developed country contexts, E-waste accompanies a wide list of pathways that involve formal as well as informal recycling, storage, and dumping. Taking into account this globally, the regulation of e-waste as a hazardous stream has undergone notable changes in the past decade. Many developed and developing countries have been involved in extended producer responsibility laws where the electronic manufacturers are made to pay for a proper recycling system for the disposal of these electronics[7].

[6] Vanessa Forti, Cornelis Peter Baldé, et.al The Global E-waste Monitor 2020, ISBN Digital: 978-92-808-9114-0, available at https://www.itu.int/en/ITU-D/Environment/Documents/Toolbox/GEM_2020_def.pdf

[7] Shagun, Ashwani Kush, and Anupam Arora, Proposed solution of E-waste management-; International Journal of Future Computer and Communication, Vol. 2, No. 5, October 2013 http://www.ijfcc.org

Based on the recent records about 75% of the e-waste is not serving its purpose in finding ways to use them for refurbishment, remanufacture and reuse the parts, etc. Toxic materials such as leaded glass, mercury lamps, etc, are exported by recyclers to developing countries due to their cheap labour. Third world countries consume this e-waste from Europe and the USA due to their poverty and for a livelihood. Dismantling, refurbishing, and remanufacturing valuable metals and establishing PVC coating for wires produces hazardous smoke and huge amounts of carbon particles which may cause lung and skin cancer. In 2018, a study conducted by The Associated Chamber of Commerce and Industry of India(ASSOCHAM) and KPMG ranked The United States as the first in e-waste generation. It generates 20 million tonnes of e-waste annually. followed by this, China ranked second with the production of 10 million tonnes of e-waste every year. There were other countries such as Japan, India, Germany, Brazil, Russia, and many other countries who are producers of e-waste in the world. More than 95% of e-waste is treated and recycled in urban slums of the country, where the process of these is carried out mostly by untrained workers without personal protective gadgets. The e-waste is either disposed of or stored in certain warehouses or exported to countries such as China, India, Ghana, and Nigeria. And from these countries, they are recycled through informal recyclers who use low-tech methods like manual dismantling, open burning, and acid leaching. This causes personal health issues and also various environmental pollution to the surroundings as well[8].

Based on European Environment Agency, 1.3 million tons of e-waste are exported from different countries mainly from Africa and Asia. In 2003, more than 23,000 metric tons of e-waste which are undeclared from the United Kingdom were illegally exported to India.. In 2005, 18 European seaports were inspected and among this 47% of e-waste has not been legally exported. 8% of the global e-waste has been generated from the United States and the majority of this has not been registered.

LEGAL REGIMES IN INDIA

[8] Ms Akanksha Manish and Dr Paromita Chakraborty, E-Waste Management in India: Challenges and Opportunities, 6 Nov2019, published by The energy and Resource Institute.

The Constitution of India considers solid waste management as a primary liability to the Municipalities under the Twelfth Schedule. Article 243W[9] empowers the State Legislatures to frame legislations in respect of waste management. The Municipal Solid Wastes (Management & Handling) Rules, 2000 were enacted by the Central Government which deals with such issues of management among which it also considers e-waste to an extent. Being the parent statute, the Environment Protection Act, 1986 is of prime importance as it confers on the Central Government, the power to take all the necessary measures as it deems fit for protecting and improving the quality of our environment and adopt methods to control and prevent environmental pollutions to a greater extent.

The Hazardous Wastes (Management, Handling, and Trans-boundary Movement) Rules, 2008

The Central Government drafted the Hazardous Material (Management, Handling, and Trans-boundary Movement) Rules, 2007 to prohibit cross-border movement of hazardous waste as suggested by the Basel Convention[10]. It included directions for the management and handling of hazardous wastes. According to the rules, every person desirous of remanufacturing perilous waste together with electronics and electrical waste is required to register with the Central Pollution Control Board. Under the Hazardous Waste (Management, Handling, and Trans-boundary Movement) Rules, 2008, the Ministry of Environment and Forests is the nodal Ministry that deals with the cross-border movement of hazardous wastes. It has divided the items that can be transported into three categories i.e., compounds that can be trade-in with prior approval, free imports under Open General License, and compounds that are prohibited for import in India.

The E-waste (Management) Rules, 2016

In India, the management of electronic waste has been considered of prime importance since the 2011 role of which the E-waste (Management) Rules, 2016 is of greater importance. There were certain drawbacks that arose after the enactment of the 2011 rules; some of them were based on the ignorance of the unorganized, small, and medium sectors and informal manufacturing units in India. Various studies revealed that these unorganized sectors contributed

[9] Article243 W, Powers, authority and responsibilities of Municipalities
[10] Available at http://www.basel.int/Implementation/Ewaste/Overview/tabid/4063/Default.aspx

about 90 percent to perilous waste disposals. Based on a study conducted by the Electronics Industry Association of India in support of the Department of Scientific and Industrial Research, Ministry of Science & Technology, on the status of e-waste management prevailing in India proved that a symbiotic relationship between the formal and the informal segment was crucial. It thereby led to the enactment of the 2016 rules.

The Ministry of Environment, Forest, and Climate Change notified the E-Waste Management Rules, 2016 on 23 March by replacing the e-waste (Management & Handling) Rules, 2011. They were introduced to enable the reuse of useful material from the discarded electronic, electrical waste, thereby reducing reckless disposal thereby ensuring the safety and environmentally-friendly handling, transporting, storing, and recycling of e-waste.

The amended rules were a major breakthrough as it extended its purview to components or consumables or parts or spares of Electrical and Electronic Equipment (EEE), along with their products. It strengthened the Extended Producer Responsibility (EPR) and introduced the Producer Responsibility Organization (PRO). PRO is a professional organization that would be authorized and financed collectively or individually by producers, to share the responsibility for collection as well as channelization of e-waste generated from the 'end-of-life' products thereby ensuring proper management of such electronic waste without endangering the environment. The adoption of collection centers and collection points were introduced in order to collect the discarded material as part of EPR. The rule included a list of equipment under Schedule I and also extended the applicability of the rules to spares and other components.

The Rule also deals with the producer of electrical and electronic equipment and their components shall ensure that new equipment does not contain pollutants like lead, mercury, cadmium, etc. beyond a maximum prescribed value. And every producer should provide detailed data about the components of the product. And also it has to be produced with a confirmation of Restriction of Hazardous Substances provisions[11].

[11] Hazardous and other wastes (Management and Transboundary movement) Rules2015; the Gazette of India Extraordinary, Part II, Section 3 Sub Section (i), New Delhi, Ministry of Environment and Forests Notification, New Delhi (April 4, 2016).

Central Pollution Control Board shall carry out specific sampling of electronic equipment that is placed on the market so as to monitor and verify whether the producer has complied with the provisions of the same and if not the producers shall take corrective measures and recall the product from the market, within a reasonable period as per the guidelines of the pollution control board. Schedule III of the Rules prescribes the collection and channelization of e-waste in Extended Producer Responsibility.

ISSUE WITH THE MANAGEMENT

Due to the strong penetration of technological advancement and economic growth, the usage and thereby wastage of electronic waste is high. Lakhs of people working in the unorganized sector of e-waste disposal are often exposed to chemicals while processing and dismantling these materials. Apart from toxic substances they also contain valuable substances like gold, silver, copper, etc. Today's world is witnessing a development coupled with e-waste generation. There are mainly four methods adopted for dealing with the same, such as; dumping in landfills, incineration, reusing, and recycling. In India, there are poor management strategies adopted for coping with the scenario. We do not have proper well-developed collection centers across the country or in most situations they are dominated by the informal sectors. There is a greater chance of non-compliance with management regulations and violation of Article 24 of the Indian Constitution by adopting forced child labour. It is a very common scene in most of the countries that children being the vulnerable section are forced to do such work. As the Government of India has imposed 12 percent of Goods and Service Tax on electronic recyclers it caused a deterrent impact on formal recyclers. The major issue with the matter is the lack of proper awareness among the public. The common people aren’t aware of the management strategies, they often dispose of it without proper segregations. Recycling of electronic waste is considered to be a complicated matter as most of the countries are able to recycle only 20 percent of the generated waste. The prevailing e-waste management rule has various loopholes such as; there is no specific monitoring mechanism in order to ensure whether the collected e-waste reaches the authorized dismantlers or recyclers. As a result, a large amount of e-waste is treated in environmentally unstable manners. Secondly in spite of the legislations that prohibit the

import of e-waste in India, wide ranges of e-waste are being illegally transported by other developed countries[12].

THE ROAD YET TO BE TAKEN

In a country like India, people are becoming conscious about managing their household waste and are adopting methods like biogas, composting, etc., but at the same time are neglecting the management of e-waste. It is a matter of great disquiet that the people are unaware of the hidden traumas that can be caused by the reckless disposal of electronic waste. There are various methods by which e-waste can be reduced. The first important method is by adopting recycling techniques[13]. As the manufacturers try to concentrate on reducing the lifespan of their products in order to maximize sales and demand, there is a higher need for well-established recycling units in both formal and informal centers with highly invested collection centers. By comparing the varieties of e-waste, our country lacks well-furnished legislation to deal with the gradual accumulation of new categories of e-waste. For example, the matters pertaining to the management of electronic waste materials from solar and photovoltaic cells are not specified under the legislation.

The Government should implement more stringent rules and completely ban the import of e-waste and there should be a more domestic legal framework so as to address the gap created. There should be the proper linkage of activities carried on in between informal and formal recycling units. Tax incentives should be provided for scrap dealers and also initiatives should be taken to impart more concentration on recycling technologies in India. Modern methods can be adopted all over India such as bioremediation. It is a general concept where the land is treated that has already been contaminated to its original state. In the presence of these electronic scraps, bacterias like Thiobacillus, Thiooxidans, fungi- Aspergillus, Penicillium grow in its presence. The formation of inorganic and organic acids caused the mobilization of metals. There are other methods such as Landfilling, Incineration, and Recycling that helps in the safe disposal of e-waste without causing environmental distress. Products that are made out of plastic can be

[12]Monika and Jugal Kishore, E-Waste Management: As a Challenge to Public Health in India, PMCID: PMC2963874, Indian J Community Med. 2010 Jul; 35(3): 382–385. doi: 10.4103/0970-0218.69251
[13] Samar Lahiri, Recycling of E-waste in India and its potential. Published on 17th April 2019 https://www.downtoearth.org.in

recycled by using the "shredding and melting" method. Printed circuit board waste such as those used for fire inhibitors and for other electronic parts; can be disposed of by desoldering and open burning so as to remove metals. Other miscellaneous waste such as chips, electronic wires, broken glass waste, or any copper-containing waste can be disposed of by chemical stripping and open burning. Liquid waste on the other hand is treated by sewerage systems[14].

In essence, the main recycle and recovery steps for safe and effective disposal of e-waste includes:

- Dismantling
- Segregation of ferrous metals, non-ferrous metals and plastic
- Refurbishment and reuse
- Recycling or recovery of valuable materials
- Treatment or disposal of dangerous materials and waste

CONCLUSION

The rapidly growing waste has become a major problem as it has great repercussions on natural resources, human beings, and our environment. By not adopting proper management techniques we are digging our own graves. Industrialization and globalization enhanced the hyper-consumption of products that tends to meet our demands and make our life easy. Apart from various legal regimes that prevail all over the world dealing with the menace of improper treatment of e-waste, it still remains as the elephant in the room. It is highly crucial to have proper channelizing methodologies adopted among the informal and formal sectors in our country. It can go a long way in reducing environmental degradation by open burning and haphazard landfilling. It is the need of the hour for developing and underdeveloped countries to adopt proper well-furnished schemes and campaigns that endorse the mechanism for handling and treating these electrical and electronic gadgets in a proper manner thereby making them further use. Reuse and recycling is the effective and convenient alternative that can be offered in order to reduce the amount of toxic and hazardous substances entering into the environment

[14] CPCB. Guidelines for environmentally sound management of e-waste (As approved vide MoEF letter No. 23-23/2007-HSMD) Delhi: Ministry of Environment and Forests, Central Pollution Control Board, March 2008. Available from: http://www.cpcb.nic.in

TECHNOLOGICAL PERSPECTIVES OF MEDIA LAW

Tejaswini Sinha[1]

ABSTRACT

The Internet brings chance and peril for media freedom and freedom of expression. It permits new types of publication and extends the reach of ancient publishers, however its power will increase the potential injury of harmful speech and invitations, state regulation and censorship still as well as manipulation by personal and business interests.In jurisdictions round the world, courts, lawmakers and regulators grapple with these contradictions and challenges totally different in several in numerous} ways with different goals in mind. The media law reforms area unit they're} adopting or considering contain crucial lessons for those forming their own responses or UN agency requests to grasp however technology is driving such speedy modification in however info and opinion are distributed or restricted.Mass Media systems of the planet vary from one another in keeping with the economy, polity, faith and culture of various societies. In societies that followed communism and totalitarianism, just like the former land and China, there have been limitations of what the media may say concerning the government. virtually everything that was aforementioned against the State was expurgated for worry of revolutions. On the opposite hand, in countries like the USA, that have a Bourgeois Democracy, virtually everything is allowed.

This article traces the developments of media technology by lightness of the crucial drone controversies. First, it'll trace the event of contemporary journalism and also the use of drones in news gathering. Next, it'll discuss the policy and constitutional considerations ensuing from the employment of media technology in newsgathering and dissemination. Finally, it'll analyze the theories of technological regulation, resting on a reformed approach to media technology law and judicial proceeding. the present state of affairs necessitates a lot of relevant litigations and a lot of malleable judges so as to progress a lot more steadily into the longer term..

[1] KLE LAW COLLEGE, BANGALORE.

The birth of the digital age brought with it a pace evolving news gathering and distribution method. Rather than looking forward to the delivery of the native newspaper customers area unit perpetually connected to a world net of instant news dissemination. Retweeting content and posting concepts on an os forum have replaced clipping writing from the paper and writing a letter to the editor. The advancements of media technology manufacture complicated legal problems, difficult precedent before a far a lot of stagnant professions.

INTRODUCTION

Technology and also the media square measure interlinking, and neither may be separated from modern society in most developed and developing nations. Media could be a term that refers to any or all print, digital, and electronic means that of communication. From the time the machine was created (and even before), technology has influenced however and wherever data is shared. Today, it's not possible to debate media and also how societies communicate while not addressing the fast-moving pace of technology. Twenty years past, if you wished to share news of your baby's birth or employment promotion, you phoned or wrote letters. you may tell a couple of individuals, however, in all probability you'd not decision up many hundred, together with your recent high school chemistry teacher, to allow them to apprehend. Now, by tweeting or posting your massive news, the circle of communication is wider than ever. Therefore, we tend |once we|after we} cite however societies have interaction with technology we should take media under consideration and the other way around.

Technology creates media. The magazine to procure your girl at the pharmacy could be a style of media, as is that the picture show you rented for family night, the net web site you accustomed order dinner on-line, the hoarding you passed on the thanks to getting that dinner, and also the newspaper you browse whereas you were waiting to select up your order. while not technology, media wouldn't exist; however bear in mind, technology is over simply the media we tend to square measure exposed to.

New media encompasses all interactive forms of information exchange. These include social networking sites, blogs, podcasts, wikis, and virtual worlds. The list grows almost daily.

New media tends to level the playing field in terms of who is constructing it (i.e., creating, publishing, distributing, and accessing information) (Lievrouw and Livingstone 2006), as well as offering alternative forums to groups unable to gain access to traditional political platforms, such as groups associated with the Arab Spring protests (van de Donk et al. 2004). However, there is no guarantee of the accuracy of the information offered. The immediacy of new media coupled with the lack of oversight means that we must be more careful than ever to ensure our news is coming from accurate sources.

New media is already redefining information sharing in ways unimaginable even a decade ago. New media giants like Google and Facebook have recently acquired critical manufacturers in the aerial drones market creating an exponential ability to reach further in data collecting and dissemination. While the corporate line is benign enough, the implications are much more profound in this mostly unregulated arena of aerial monitoring. With claims of furthering remote internet access, "industrial monitoring, scientific research, mapping, communications, and disaster assistance," the reach is profound (Claburn 2014). But when aligned with military and national surveillance interests these new technologies become primarily exempt from regulations and civilian oversight.

Today, the net is employed to access felonious gambling and erotica sites, moreover, on analysis stocks, crowd-source what automotive to shop for, or detain bit with childhood friends. will we tend to enable one or a lot of these activities, whereas proscribing the rest? And the UN agency decides what it wants to restrict? associate exceedingly In a very country with democratic principles and an underlying belief in free-market free enterprise, the solution is determined within the court system. however globally, the questions—and the government's responses—are different.

It is troublesome to create by mental act any one theory or theoretical perspective which will justify the variability of the way that individuals move with technology and also the media. Technology runs the gamut from the match you strike to lightweight a candle all the far too stylish nuclear energy plants that may power the manufacturing plant wherever that candle was created. Media might discuss with the tv you watch, the ads wrapping the bus you're taking to

figure or faculty, or the magazines you flip through in an exceeding room, to not mention all the styles of new media, as well as Twitter, Facebook, blogs, YouTube, and also the like. Are media and technology crucial to the forward march of humanity? area unit they pernicious capitalist tools that cause the exploitation of employees worldwide? area unit they the remedy the globe has been expecting to level the taking part in field and lift the world's poor out of utmost poverty? every perspective generates understandings of technology and media that facilitate the U.S. examine the method our lives area unit affected.

China is in some ways the worldwide tiddler for the uncomfortable relationship between web freedom and government management. a rustic with a good rein on the dissemination of data, China has long worked to suppress what it calls "harmful data," as well as dissent regarding government politics, dialogue regarding China's role in an Asian country, or criticism of the government's handling of events.

With sites like Twitter, Facebook, and YouTube blocked in China, the nation's web users—some five hundred million sturdy in 2011—turn to native media firms for his or her wants. Renren.com is China's answer to Facebook. maybe a lot of significantly from a social-change perspective, Sina Weibo is China's version of Twitter. Microblogging, or Weibo, acts like Twitter therein users will post short messages which will be browsed by their subscribers. and since these services move thus quickly and with such wide scope, it's troublesome for state overseers to stay up. This tool was wont to criticize government response to a deadly rail crash and to protest a manufactory. it was additionally attributable to the government's call to report a lot of accurately on the pollution in the capital of Red China, which occurred when a high-profile campaign by a widely known property developer (Pierson 2012).

There is absolute confidence in China's authoritarian government ruling over this new kind of web communication. the state blocks the employment of bound terms, like "human rights," and passes new laws that need folks to register with their real names, creating it a lot dangerous to criticize government actions. Indeed, 56-year-old microblogger Wang Lihong was sentenced to 9 months in jail for "stirring up hassle," as her government delineates her work serving to folks with government grievances (Bristow 2011). however the govt. cannot finish off

this flow of data fully. Foreign firms, seeking to interact with the more and more vital Chinese shopper market, have their accounts: the NBA has quite five million followers, and doubtless, the foremost illustrious foreigner in China, Canadian comedian, and Order of North American country recipient Mark Rowswell boasts nearly three million Weibo followers (2014). the govt., too, uses Weibo to induce its message across. because of the years' progress, the remainder of the globe uneasily watches China's approach to social media and also the freedoms it offers—on Sina Weibo and beyond—the remainder of the globe.

The issue of censorship of online content in Asian nations could be a tough one as" the Constitution permits censorship in bound restricted circumstances. This is often a haul as thanks to the worldwide nature of the web, it's troublesome to regulate content being uploaded in foreign countries and being viewed in Asian nations. Further, the thorny issue of WHO gets to decide to censor content beneath what circumstances could be a nuanced dialogue " that sadly tends to be hijacked by arguments supporting security issues / would like for broad emergency provisions. Most tries at censorship have so been haphazard and inconsistent. This paper seeks to critically analyze that.

India, like all countries, is more and more facing a state of affairs wherever legal frameworks that created sense before the explosive growth of the web are proving incomplete or in some cases being repurposed as blunt instruments of state power. Reforms are desperately required, and therefore the pressure for reform begins with awareness. This is often the primary in a very series of posts seeking to boost a well-liked understanding of problems with Indian law.

The past few years have seen Associate in Nursing explosion in web usage in Asian nations with roughly a tenth of the country's population currently thought-about active web users. whereas the accrued access to and use of on-line resources is doubtless helpful to the country as a full, there still stay varied shortcomings starting from lack of access in rural areas, inclined sex ratios of these accessing the web, and lack of adequate infrastructure, etc. There also are issues with the legal framework governing the web scheme in Asian nations that have captured public attention over the last 2 years, with the media focusing notably on censorship and police investigation.

Censorship beneath The It Act:

Indian law concerning censorship in ancient media is fairly developed and comparatively liberal (at least in theory). Article 19(1)(a) of the Constitution protects the proper to free speech and expression no matter the medium of communication. whereas the Courts have taken this right in a very broad manner, Article 19(2) permits affordable restrictions to be placed on the proper insight of public policy issues.

Purportedly following A 19(2), the IT Act contains varied provisions which will be accustomed censor online content" notably in Sections 66A, 69A, and 79. Most tellingly the majority of these instances involve government action with no system of judicial oversight â€" really beneath Section seventy-nine, the law actively encourages non-public censorship. Section 66A has in all probability received the foremost media attention over the last year close to thanks to the numerous arrests created beneath this section (notably the arrest of 2 adolescent women in Palghar, the geographic area in Nov 2012. This provision criminalizes the follow of causation Associate in Nursing offensive message employing a pc resource. The most important concern during this regard is that the very wide and ambiguous scope of the availability that may embody something that's thought-about offensive, menacing, that causes annoyance or inconvenience, that insults, that causes enmity, emotion or ill-will, etc. The social control for such an Associate in Nursing offense is 3 years imprisonment.

The wide phrasing of the availability has ensured that it is accustomed to criminalize virtually any behavior on the web (including that which might not represent against the law within the physical world) and this has been seen in following as varied activists and different are inactive for posting comments important of political parties or persons (usually, as illustrated by the aforesaid Palghar case, for posting fully innocuous comments). The widespread public uproar following the many instances of misuse of this provision results in a Public Interest petition being filed in Indiaâ€™s Supreme Court, that browses down the availability holding that the powers beneath the section (of arrest) were to be used solely upon directions from a senior police official. the availability but continues to stay on the statute books.

Two different sections of the Act - Section 69A and seventy-nine have received so much less attention from the general public, presumably as these are substantive provisions of law and not penal provisions (as S 66A is). These provisions but found a system of censorship that's arguably unconstitutional.

S 69A authorizes the government to dam any content from being accessed by the general public on varied grounds. Associate in Nursing mediator WHO fails to fit directions to dam content is at risk of being unfree for up to seven years.

This provision ensures that the govt will block any content it deems to fall inside the fairly broad conditions and has been used with mixed results â€“ whereas little question there are instances wherever content will be expurgated (for instance one in all the sparks for the recent communal violence in the state was the distribution through Facebook of a faux video supposedly showing violence committed against the bulk community), follow shows that directions issued by the govt lack exactness (leading to whole domains and websites being blocked) lack applicable oversight and responsibility mechanisms, etc. The broad and ambiguous nature of the conditions to be glad before invoking this power also are cause for concern.

Section seventy-nine of the IT Act needs an Associate in Nursing intercessor to watch bound pointers to avail of the exemption from liability. These pointers (issued in 2011) mandate that the intercessor should take down any info that's put down Alia grossly harmful, harassing, blasphemous, defamatory, obscene, sexy, paedophilic, libelous, invasive of another's privacy, hateful, or racially, ethnically objectionable, derogative, relating or encouraging hiding or gambling, hurt minors in any means or otherwise unlawful in any manner no matter, acting upon personal criticism or if they discover such content on their own.

This provision makes all intermediaries into watchdogs of the web with terribly restricted provisions on a recourse or safeguards " for example, there's no demand to supply a writ before (or after) mandating a takedown. the need to act on personal criticism for such a good sort of â€˜offencesâ€™ (some of that once more don't seem to be crimes within the physical world â€“ for example blasphemy isn't a criminal offense in India) is perturbing and will be used as a back-door suggests that of censorship. This method additionally sets up Associate in Nursing alternate

systems of criminal offenses and censorship for on-line media as against ancient media (therefore a physical newspapfffer will carry a piece questioning the existence of God whereas its on-line version cannot!).

Various organizations are candidacy for Associate in Nursing modification to the current provision and truth the Parliament Subordinate Committee on Legislation has counseled revisiting these pointers to form them compliant to the Constitution. more steps square measure nonetheless to be taken by the govt, which has, however, assured the country that it's not fascinated by censoring content.

The social media law Republic of India is regulated by the Data Technology Act that was enacted within the year 2000 to control, management and traumatize the problems arising out of IT. Social networking media is Associate in Nursing â€œintermediaryâ€ inside the means of Indian info technology act 2000 (IT Act 2000). so social networking sites in India square measure responsible for numerous acts or omissions that square measure punishable below the laws of India.

Section 66A of the IT Act has been enacted to control the social media law of India country and assumes importance because it controls and regulates all the legal problems associated with social media law in India. This section restricts the transmission, posting of messages, emails, comments which may be offensive or unwarranted. The violative message will be in some sort of text, image, audio, video, or other electronic records that is capable of being transmitted. Within the current eventualities, such sweeping powers below the IT Act provides a tool within the hands of the government to curb the misuse of the Social Media Law Republic of India in any type.

However, in 2015, during a landmark judgment upholding the correct to free speech in recent times, the Supreme Court in Shreya Singhal and Ors. Vs Union of the Republic of India, struck down Section 66A of the data & Technology Act, 2000. The ruling that is being lauded by the individual and legal luminaries alike, found the Cyberlaw provision to be open-ended, imprecise, and unconstitutional because of the restriction it caused to the Indian citizen’s right to free speech.

The repeal of S.66A doesn't but lead to Associate in Nursing unrestricted right to free speech since analogous provisions of the Indian legal code (IPC) can still apply to social media on-line viz. by choice Insulting faith Or nonsecular Beliefs, Promoting Enmity Between teams On Grounds of faith, Race Etc ., Defamation, Statements conducing to Public Mischief, Insulting The Modesty Of a lady, Criminal Intimidation (S 506), etc.

Conclusion:

The issue of censorship of online content in Bharat may be a difficult one â€“ the Constitution permits censorship in bound restricted circumstances. This is often a retardant as thanks to the world nature of the net, it's troublesome to manage content being uploaded in foreign countries and being viewed in Bharat. Further, the thorny issue of WHO gets to decide to censor content and beneath what circumstances may be a nuanced discussion â€“ that sadly tends to be hijacked by arguments supporting security issues/want for broad emergency provisions. Most tries at censorship have thus been haphazard and inconsistent.

Further, problems raised by communal, harmful, and violent content (particularly towards women) still receive little or no attention. notably worrying is that the lack of responsibility, transparency, and oversight within the system. One hopes that the Supreme Court can take acceptable action by putting down the relevant provisions within the IT Act thereby forcing the assembly and government to place in situ a lot of open, equitable, and simple systems of censorship that abides by the Constitutional spirit embodied during 19(1)(a)

TELEMEDICINE AND DATA PRIVACY OF PATIENT: SINE QUA NON FOR REFORMING HEALTH SERVICES

Mukul Bhutda[1] Nikita Jain[2]

"Telemedicine will become the core methodology of healthcare delivery in the future. That is where we are going to get the efficiencies, we need to provide affordable care".

--Yulun Wang

ABSTRACT

Telemedicine means 'healing from a distance'. Telemedicine is contemplated as revolutionary and at present, it is a paramount mechanism for expedient as well as specialized healthcare, specifically for patients in remote locations with limited access to standardized healthcare services. Therefore, this research paper will ventilate the numerous dimensions where telemedicine is beneficent. However, despite having a lot of benefits, it also has some serious issues like breach of Data privacy of the Patient and the present study will inquisitively enclose the significance of this breach of Data privacy of patient. Furthermore, a strenuous attempt to check the massive impact of the data privacy breach on health and economic indicators. The research paper will examine the challenges in realizing the full potential of telemedicine, telehealth and e-health in India. Further, the authors will review India's pharmaceutical regulatory environment's pertaining about the application of telemedicine, telehealth and e-health. A laborious effort will be made to check the various challenges faced in implementing the current legislature. The author will also analyze the surges in current state of the utilization of telemedicine, telehealth and e-health amid the current COVID-19 pandemic and to evaluate the drawbacks of continuing telemedicine usage during COVID 19 which results in data privacy breach of the patient. Furthermore, a study is also conducted on some International Jurisdictions to showcase their steps in reforming their respective statutes for safeguarding the public health issue due to data privacy breach. In the concluding part, an effort will be made to provide some suggestions for the amelioration of Medication system in India and curbing breach of Data privacy of the patient.

[1] Student School of Law, University of Petroleum and energy studies, Dehradun.
[2] Student School of Law, University of Petroleum and energy studies, Dehradun.

I. INTRODUCTION:

Along with the emergence of information technology, the nation has attempted to revise itself to accommodate humans' requirements. Initially, patients had to travel to far-off places to avail themselves of medical services, but now with technological advancement, this lengthy process can be simplified. Besides, there are significant medico-legal issues regarding e-health services in India, like registration to privacy, confidentiality issues of the patient, and other risks associated with electronic health care communication. Apart from that, one more aspect of this which needs cogitation is that what should be the degree of vigilance that can be anticipated from a doctor.

- ***Elucidation of the term 'Telemedicine'* and *'Telehealth':***

Telemedicine, a term coined in the 1970s, literally means "*healing at a distance*[3]."According to the **World Health Organization**, "The delivery of health care services, where distance is a critical factor, by all health care professionals using information and communication technologies for the exchange of valid information for the diagnosis, treatment, and prevention of disease and injuries, research and evaluation, and for the continuing education of health care providers, all in the interests of advancing the health of individuals and their communities[4]."

The locution '*Telemedicine*' is different from the term '*Telehealth*'. Primarily, telemedicine is accustomed to denote clinical service delivered by a registered medical practitioner. Simultaneously, telehealth is a broader term of use of technology for health and health-related services, including telemedicine[5].

[3]Strehle EM, Shabde N., One hundred years of telemedicine: does this new technology have a place in pediatrics?, (2006). Arch. Dis. Child. 956.
[4]A health telematics policy in support of WHO's Health-For-All strategy for global health development: report of the WHO group consultation on health telematics, 11–16 December, Geneva, 1997, World Health Organization, <https://apps.who.int/iris/handle/10665/63857> accessed 13 January.
[5] Indian Medical Council, Telemedicine Practice Guidelines, Appendix 5, (Issued on 25th March 2020). (Telemedicine Practice Guidelines).

Telemedicine and Date Privacy

The term '***Telehealth***' connotes the delivery and facilitation of health and health-related services, including medical care, provider and patient education, health information services, and self-care via telecommunications and digital communication technologies[6]."

- ***The Legal position of E-health services in India:***

The practice of telemedicine and telehealth is not so customary and prominent in India; therefore, we don't have any specific legislation till now which administers the telemedicine and telehealth process. Initially, telemedicine governed under The Indian Medical Council Act, 1956; The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002 and Drugs and Cosmetics Act 1940. But the COVID-19 Pandemic circumstances elevate some significant concerns about the current health facilities in India. The Global lockdown undoubtedly increased the demand for Telemedicine and Telehealth services in India. It forced healthcare institutions and regulatory bodies to turn to alternative ways of providing healthcare while limiting exposure to the virus. Therefore, Telemedicine is the optimal compound that limits patient displacement to hospitals and hospital space assignment to crucial cases, which also leads to suppressing the disease's spread. On that account, to avoid contact between the Registered Medical Practitioner and the patient plus to provide hassle-free routine checkup, especially to the rural people to mitigate the distance factor, The Ministry of Health under the head of Indian Medical Council issued the guidelines on 25th March2020, for governing the telemedicine practice in India by the Registered Medical Practitioner[7].These guidelines provide the necessary overview to deal with the practice of Telemedicine and Telehealth. However, there were many things that need to be covered and specific legislation should be enacted.

- ***The Expediency of Telemedicine:***

With respect to India, providing in-person healthcare apparatus is an arduous as well as a laborious task, on account of the substantial geographical distances and limited resources. One of the telemedicine's consider able supremacies is that it saves money and efforts, especially for patients belonging to rural areas, as they need not travel long distances for obtaining consultation and treatment in metro cities. Therefore, telemedicine and telehealth can lay out an appropriate

[6] Ibid.
[7] Ibid.

explication for providing timely and faster access for these said situations. Also, it would even lower down the financial costs associated with traveling. Apart from that, it can also lessen the disruption to the family and other caretakers of the patient. One of the most foremost benefits of Telemedicine is in cases where there is no requisite for the patient to physically meet the Registered Medical Practitioner (or another medical professional), e.g., for regular, routine check-ups or continuous monitoring. Hence, Telemedicine can also dwindle the superfluous onus on the hospitals and Registered Medical Practitioners[8]."

Noteworthy, Telemedicine will be going to assist stringently in the maintenance and alimentation of records and documentation, which, therefore, minimizes the plausibility of missing out an older prescriptions and instruction from the doctor and other health care staff. Furthermore, the doctor has an exact piece of document of the advice with accurate date, time, and credentials provided via teleconsultation. Besides, written documentation surges the legal protection for both the parties to such an extent that they both can be backed by some authentic proof, which consequently decreases the probability of arising cases of medical negligence. Telemedicine and telehealth contribute to patient's safety, especially in situations where there is a risk of contagious infections like the COVID 19 virus. There are several technologies and software's that can be used in telemedicine and telehealth, which can help the patients and health care workers to adhere better to the medication regimens, manage the diseases better and cure the patient well[9].

Nonetheless, despite having a lot of the abovementioned advantages, there have been some remarkable disquietude on the practice of telemedicine and telehealth. Lack of adequate regulations has constituted significant ambiguity for registered medical professionals, which therefore raises doubts on the practice of telemedicine.

The 2018 judgment of the ***Deepa Sanjeev Pawaskar and Anr.*** **v.** ***State of Maharashtra[10],*** where the deceased patient had propounded herself with an ailment of fever and severe vomiting. She was admitted to the nursing home of the charged specialists by the emergency clinic staff

[8] Telemedicine Practice Guidelines, 2020.
[9] Telemedicine Practice Guidelines, 2020.
[10] [2018] SCC OnLine Bom 1841.

without assessment, as the doctors were away. One of the doctors began treatment for the patient telephonically by training the on-duty nurse. Unfortunately, the patient died. Therefore, *the* Hon'ble High Court of Bombay had created uncertainty about the place and legitimacy of telemedicine because of the unavailability of an appropriate framework, although the judgment should not be concluded to affirm that the enactment of telemedicine and teleconsultation itself is illegal[11].

Till now, in India, there is no specific legislation on the practice of telemedicine which is through video, phone, Internet-based platforms. The current arrangements underneath the Indian Medical Council Act, 1956; the Indian Medical Council (Professional Conduct; Etiquette and Ethics Regulation 2002); Drugs &Cosmetics Act, 1940 and Rules 1945; Clinical Establishment (Registration and Regulation) Act, 2010; Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011,mainlyadminister the practice of medicine and information technology. Therefore, the aperture in legislation and the uncertainty of rules pose a risk for both the doctors and their patients.

There are some countries that have put telemedicine in legislative measures, and some countries follow non-legislative standards such as guidelines to practice telemedicine. In some countries, guidelines are treated as professional norms that need to be followed by medical practitioners. Telemedicine will continue to grow and be adopted by more healthcare practitioners and patients in a wide variety of forms, and these practice guidelines will be a crucial enabler in fostering growth.

II. COVID 19 AND TELEMEDICINE:

[11]**Anay Shukla, Anil Upadhyay,** ***India's new Telemedicine Practice Guidelines - Analysis and Do's and Don'ts for Doctors offering teleconsultation,*** **Lexology <https://www.lexology.com/library/detail.aspx?g=a1d76ffa-1853-4c7a-84e8-f8ef37d44525> accessed 13 January.**

Telemedicine and Date Privacy

Catastrophe and pandemics give rise to unique challenges to administering the health care system. Though telemedicine and telehealth will not decode them all, although it is well applicable for scenarios in which medical practitioners can evaluate and manage patients remotely, which saves time and efforts[12].One of the paramount benefits is that telemedicine visits can be conducted without exhibiting staff to viruses/infections. Telemedicine practice can avert the transmission of infectious diseases, which helps in reducing the risks to both health care workers and patients. Unnecessary and avoidable exposure of the people during the delivery to healthcare systems can be bypassed using telemedicine, and patients can be screened remotely. It can dispense speedy access to medical practitioners who may not be immediately available in person. Besides, it makes available extra working hands to provide physical care at the respective health institutions. Also, In India, the rural people have to suffer a lot for getting the health facilities, as they have to travel all the way from rural areas to the cities to obtain good health faculty. But for all these, we need good and very specific legislation to control and monitor all the aspects of this very critical process, and this paper attempt to cover the crucial element of that process through the eyes of the law and also this paper tries to provide some suggestion to make the process smoother lawfully. Thus, health systems that are invested via telemedicine are unencumbered to assure that patients with Covid-19 kind of issues receive the care they need[13].

Telemedicine is a modernist kind of provision of health-related services that ameliorate the standard and accessibility of health care by consolidating information and communication technologies in the health sector. The application of telemedicine services devotes to health improvement, and its application should be considered favorably. Although, it is mandatory to be acquainted that the adoption of distinct telemedicine solutions encompasses the processing of patient data. As follows, this matter should be scrutinized from the stance of data protection. Notwithstanding, the verity that telemedicine services usage will positively form changes in the relationship between the health care professional and patient should not negatively affect persons' rights to data protection. Hence, the person who receives health care services is entitled to expect that health care service will be provided with respect to human rights. The next part of

[12] Telemedicine Practice Guidelines, 2020.
[13] Telemedicine Practice Guidelines, 2020.

the paper will elaborate on the concerns about the Patient's Data Privacy with respect to telemedicine and telehealth.

III. DATA PRIVACY OF PATIENTS:

According to the Information Technology Act, 2000, "*Data means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and maybe in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer*[14]*."*According to the Personal Data Protection Bill, 2018, '**Health data'** is considered as the "*sensitive personal data*"[15] and Personal Data Protection Bill, 2018 defines '**Personal Data Breach**' as *any unauthorized or accidental disclosure, acquisition, sharing, use, alteration, and destruction, loss of access to, of personal data that compromises the confidentiality, integrity, or availability of personal data to a data principal*[16].Also, Personal Data Protection Bill, 2018 defines '**Health Data**' as *data related to the state of physical or mental health of the data principal and includes records regarding the past, present, or future state of the health of such data principal, data collected in the course of registration for, or provision of health services, data associating the data principal to the provision of specific health services.*

- ***Ammunition of Patient Data:***

Undeniably, the Privacy Standards and the Security Standards are linked together. Any health record system necessitates precautionary measures to ensure that the data is readily available as and when required and that the information is not deliberately used, disclosed, accessed, altered, or deleted inappropriately while being stored or transmitted[17]. The safety and security guidelines work together with the Privacy Standards to establish proper measures and protections. Health sector entities required to abide by the Privacy Standards must also comply with the Security Standards to ensure good ethics and conduct.

[14] Information Technology Act, 2000, s 2 (O), No. 21, Acts of parliament, 2000 (India).
[15] Personal Data Protection Bill, 2018, s 2 (35).
[16] Personal Data Protection Bill, 2018, s 2 (30).
[17] National Health Portal, Data Privacy and Security, NHP CC DC, (Issued on 03 June 2015), (Data Privacy and Security).

Organizations mandatorily have to consider several factors when adopting security measures. The decision is left on the health organization concerning the technology being used, data security software being used, etc. While deciding security measures, an association should think about its size, intricacy, and capacities; it's specialized framework, equipment, and software security abilities; the expense of specific safety measures[18].

Electronic health record and the data of the patient in online mode enable exciting advantages, the data can be forwarded in minutes to the other health care team, and the feedback can also be written on them by the Registered Medical Practitioners, but it poses various concerns even with respect to security and safety of the data of patients. It is an antiquated custom in clinical practice that a patient's confidences should be respected and unapproved revelation of clinical data be denied. This practice has gotten logically more challenging to keep up as patients' clinical data has gotten gathered in electronic media, which can be characteristically harder to adequately secure[19].”

Telemedicine's broad access capabilities could increase the number of individuals who are privy to patients' electronically transmitted medical records, sparking new fears that the information may be intercepted and misused with even greater ease. Current safeguards do not provide adequate protection[20]. Hackers, both clever outsiders as well as disgruntled insiders, can break into systems and obtain confidential information. Numerous cases of misuse of personal health information have been documented[21].

- ***Indian Health Standard***:

In the landmark case of ***K.S. Puttaswamy v. Union of India***[22]**,**it was held thatthe right to privacy is a fundamental right under Article 21 of the Constitution of India. And now, it is a priority to safeguard the fundamental rights of the patients. It is the responsibility of the

[18] ibid (Data Privacy and Security)
[19] Kevin E. Noonan, *Personalized Medicine and Patient Privacy Concerns in the Telemedicine Age* (2017),19 DEPAUL J. HEALTH CARE L. 1.
[20] Christina M. Rackett, *Telemedicine Today and Tomorrow: Why Virtual Privacy Is Not Enough* (2017), 25 FORDHAM URB. L.J. 167, (Telemedicine Today and Tomorrow).
[21] ibid (Telemedicine Today and Tomorrow).
[22] [2018] 1 SCC 809.

advocates, activists, media, etc. to make patients aware of this concern and to raise voices against the wrongdoing.

It is essential to protect the privacy of medical records because a person's medical history may incorporate higher confidential and private attribute about an individual than could be found in any other single document, and the confidentiality of the electronic medical record is not yet adequately protected[23]. The patient's right to access her health records was once a subject of considerable controversy but now has been affirmed by statute or case law in many states. Patient access to medical record information is necessary to correct any misinformation that the record might contain[24].

Data can be chased by the following few measures: –

1. *Authentication: -*

The entity which is providing services or the Registered Medical Practitioner mandatorily needs to authenticate themselves from time to time.

2. *Automatic log-off: -*

After a meeting is finished or ended, it should be coercively logged off to prevent abuse Implementation Guideline: The ISO 27799 is given as an essential warning norm for security the executives. Other security management and standard/practices/rules given by Law, (for example, IT Act 2000 and amendments) or administrative/statutory/certification bodies, (for example, National Accreditation Board for Hospitals and Health care Providers (NABH)) should be taken into consideration when designing and/or implementing health record system[25].

3. *Access control: -*

Every time the entities and the patients need to provide specific identities or numbers in order to track user identity and establish the control of authorized users.

[23] Chari J. Young, *Telemedicine: Patient Privacy Rights of Electronic Medical Records*, 66 UMKC L. REV. 921 (1998).
[24] Terri Finkbine Arnold, *Let Technology Counteract Technology: Protecting the Medical Record in the Computer Age* (1992), 15 Hastings Comm. & Ent. L.J. 455.
[25] Data Privacy and Security.

4. *Access privileges: -*

Implementation Guideline: The ISO 22600 arrangement of norms is given as an advisory standard to strategy-based admittance control. For the purpose of privilege management, rule / policy-based access is expected to give better control and flexibility in defining and enforcing access. Access control mechanism, for example, Role-Based, Policy-Based, or particular/singular client (applicable in case of mobile-based PHR) are worthy as long as conformant to appropriate information security law(s) and rules as well as the policy of the organization where implemented.

5. *Audit login: -*

All specified actions and electronic data of patients need to be recorded with a due date, time, day, patient number, etc., in order to keep a record for securing the transaction details for use in the mere future.

6. *Encryption: -*

It is the most crucial part; all the information must be encrypted between the parties only. Secure transmission standards must be provided for the whole private session.

7. *Integrity: -*

The data must not be altered in transit; all alteration needs to be precisely detected. A secure hashing algorithm must be used to corroborate that health information has not been changed in transit.

8. *Digital certificates: -*

The use of these certificates is recommended in the health record system.

9. *Administrative safeguard standards[26]: -*

To comply with the Administrative Safeguards, a medical services provider should implement the accompanying principles.

[26] Data Privacy and Security.

- The security management process standard, to prevent security violations;
- Assigned security responsibility to identify a security officer;
- Workforce security, to determine e-PHI user access privileges;
- Information access management, to authorize access to e-PHI;
- Security awareness training to train staff members in security awareness;
- Security incident procedures, to handle security incidents;
- A Contingency plan to protect e-PHI during an unexpected event; and
- Evaluation, to evaluate an organization's security safeguards.

10. *Physical Safeguard Standards*[27]*: -*

The required physical standards are:

- The facility access control standard, to restrict genuine actual physical access to electronic data frameworks and the facilities where they're found;

- The workstation utilizes standard, to control the actual attributes of a particular workstation or group of workstations, to boost security;

- The workstation security standard, to implement physical protections to deter the unapproved access of a workstation; and
- The device and media control standard to control the movement of any electronic media containing ePHI from, to, or within the facility.

There are 3 entities that have responsibility for maintaining the confidentiality of patient medical records and other information[28]: -

- A covered healthcare provider, who is a person, business, or agency that furnishes, bills, or receives payment for health care in the ordinary course of business and transmits any covered transaction electronically[29].

[27] Data Privacy and Security.
[28] Data Privacy and Security.
[29]Elizabeth Snell, *Breaking Down HIPAA: Health Data Encryption Requirements*, HEALTHITSECURITY.COM <https://healthitsecurity.com/news/breakingdown-hipaa-health-data-encryption-requirements> accessed 13 January, (Breaking Down HIPAA).

- A health care clearinghouse, which is a business or agency that processes or facilitates the processing of health information from a nonstandard format or content into a standard format or vice versa, or the business or agency performs this function for another legal entity[30].
- A private benefit plan, which is a plan for an individual, group or some combination thereof, and provides or pays for the cost of medical care, having greater than 50participants and that is not self-administered[31].
- The Registered Medical Practitioner along with the service provider who is the part of that process.

On 25th March 2020, the Government of India, released the guidelines pertaining to the practice of telemedicine in India to maintain high standards of professionalism.

The Telemedicine Practice Guideline covers the data protection part under guideline 3.7.1[32] as: MEDICAL ETHICS, DATA PRIVACY &CONFIDENTIAILITY: --

- Principles of medical ethics, including professional standards for ensuring patient privacy and confidentiality according to the IMC Act, will be restricting and should be maintained and practiced.

- Registered Medical Practitioner would be needed to completely maintain Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002 and with the pertinent arrangements of the IT Act, Data protection and privacy laws or any relevant rules notified from time to time for ensuring patient privacy and confidentiality and in regards to the taking care of and transfer of such personal information regarding the patient. This shall be binding and must be upheld and practiced.

- Registered Medical Practitioners won't be considered responsible for breach of secrecy if there is reasonable proof to accept that patient's privacy and confidentiality has been

[30] ibid (Breaking Down HIPAA).
[31] ibid (Breaking Down HIPAA).
[32] Telemedicine Practice Guidelines.

undermined by a technology breach or by an individual other than RMP. The RMPs ought to ensure a reasonable level of care while recruiting such services.

It also elaborates that "*it is the responsibility of the RMP to be cognizant of the current Data Protection and Privacy laws. RMP shall not breach the patient's confidentiality akin to an in-person consultation. For example: If the RMP is planning to create a virtual support group for disseminating health education for patients suffering from a particular disease condition, then he/she shall be wary of the patient's willingness and not the violate patient's privacy and confidentiality by adding them to the group without their consent."*

It also defines the various misconduct that can be done and also provides examples such as - RMPs misusing patient images and data, exceptionally private and sensitive (e.g., RMP uploads an explicit picture of a patient on social media, etc.), etc.[33]And for any misuse, the penalty should be given according to the Indian Medical Ethics professionals.

Everybody obeys responsibility towards the patient; otherwise, he /she has to face the consequences.
To chase the data of patients being misused, we need to provide a specific code of telemedicine, only guidelines cannot cover all the aspects of such a big project.

- ***Legal implications of data privacy:***

Excessive use of Teleassistance, when there is neither an emergency nor medical isolation, is dangerous as it may affect the traditional medical act's integrity and quality. In normal circumstances, medical practice without any clinical examination of the patient is contrary to medical ethics[34]. Telemedicine generates a lot of concern about the validity, authenticity, credibility, and accountability of all the service providers. The guidelines reflected that in order to mitigate this, the Registered Medical Practitioner has to tell the license number plus the unique code for the purpose of corroborating[35] and on the patient side, the person has to tell the date of

[33] Telemedicine Practice Guidelines.
[34] Luv K. Sharma, Meena Rajput, *Telemedicine: Socio-Ethical Considerations in the Indian Milieu* (2009), 77 MEDICO-LEGAL J. 61.
[35] Telemedicine Practice Guidelines Guideline 3.2.

birth or other credentials as deem fit to check the person behind the screen is the same as the other one is thinking, and for issuing a prescription, the RMP needs to explicitly ask the age of the patient, and if there is any doubt, seek age proof. Where the patient is a minor, after confirming the age, teleconsultation would be allowed only if the minor is consulting along-with an adult whose identity needs to be ascertained[36]". A RMP ought to check and affirm the patient's identity by name, age, address, email ID, telephone number, registered ID, or some other ID as might be considered to be suitable. The RMP ought to guarantee that there is an instrument for a patient to check the credentials and contact subtleties of the RMP[37]. Each RMP will show the registration number agreed to him/her by the State Medical Council/MCI, on prescriptions, site, electronic correspondence (WhatsApp/email, and so forth) and receipts, and so on given to his/her patients[38]. Also, the guidelines gave clear instructions with respect to the data records.

- ***Right to health as a fundamental right:***

Registered Medical Practitioner was charging consultation fees in 3- 4 digits6[39]which consequence in the reduction of medical treatment to poor and lower-middle-class people. Article 21 of the constitution enunciates that the Right to life encompasses the right to live with dignity, and this position has been laid down under various landmark judgment like in the case of ***Aruna Ramchandra Saunbagh v. Union of India[40],*** where the Hon'ble Supreme Court considers the Right to health under the preview of Article 21 of the constitution. The Infrastructure provided by the government for the health sector is not enough, and because of that, these private practitioners charge fees according to their own will. Therefore, with the forthcoming amendments in the future, there is a need to target this matter, which has become the ultimate concern for the middle class and below middle-class group as they spend around 40% of their income on the health sector.

IV. REVIEW FROM INTERNATIONAL PERSPECTIVE:

[36] Telemedicine Practice Guidelines Guideline 3.2.3.
[37] Telemedicine Practice Guidelines Guideline 3.2.2.
[38] Telemedicine Practice Guidelines Guideline 3.2.5.
[39] **Doctor Visit Charges, Medifree <https://www.medifee.com/hospitals/doctor-visit-charges/> accessed on 13th January.**
[40] [1996] 2 SCC 648.

Telemedicine and Date Privacy

The two international landmark cases cover the head of data privacy in light of international principles when they talk about the sale and use of secondary data.

- ***UNITED STATES OF AMERICA:***

The 2011 US Supreme Court Case, ***Sorrell v. IMS Health Inc***[41]**,** Contending that Vt. Stat. Ann. tit., § 4631(d), violated their first amendment rights as incorporated by the fourteenth amendment, respondent data miners and an association of pharmaceutical manufacturers sought declaratory and injunctive relief against petitioner Attorney General and other officials of the State of Vermont. The U.S. Court of Appeals for the Second Circuit held § 4631(d) violated the first amendment. Certiorari was granted". Consequently, the Sorrell and Source cases raise more broad worldwide worries of security and information assurance, from one perspective, and suitable use and secondary use of data for data mining, marketing, research, public health, and healthcare, on the other hand[42]."

CURRENT STATUS -- The Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule") sets up, unexpectedly, a bunch of public principles for the assurance of certain health data. The U.S. Department of Health and Human Services ("HHS") gave the Privacy Rule to execute the necessity of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The Privacy Rule standards address the use and disclosure of individuals' health information—called "protected health information" by organizations subject to the Privacy Rule — called "covered entities," as well as standards for individuals' privacy rights to understand and control how their health information is used. Within HHS, the Office for Civil Rights ("OCR") has responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties[43].

- ***UNITED KINGDOM:***

[41] 564 U.S. 552, 131 S. Ct. 2653 (2011).
[42] Bonnie Kaplan, *How Should Health Data Be Used? Privacy, Secondary Use, and Big Data Sales* (2016) 25 CAMBRIDGE Q. HEALTHCARE Ethics 312.
[43] SUMMARY OF THE HIPAA PRIVACY RULE, United state department of Health & human services, <Microsoft Word - MO02PBf_pdf.rtf (hhs.gov)> accessed on 20th January.

Telemedicine and Date Privacy

The United Kingdom case in 2000 ***R v. Department of Health, Ex Parte Source Informatics Ltd*[44]*,*** points to the international nature of the ethical issues. That case was decided on the grounds that selling anonymized (de-identified) data did not violate pharmacists' duty of confidentiality[45].**"** The European Court of Human Rights ('ECtHW) emphasized the importance of protecting a person's health data in ***I v. Finland in 2008***[46]. The case involved an employee of an eye clinic, formerly a patient at the clinic, whose HIV status became known to her colleagues due to free access to the patient register containing information on diagnoses and treatment[47]. The ECtHR noted in the case that the "sensitive issues surrounding this disease" would make the requirement of confidentiality particularly important in the applicant's case. This observation of the ECtHR places an obligation on data controllers to keep all confidential data safe from unauthorized access.

CURRENT STATUS -- On 25th May 2018, the EU General Data Protection Regulations (GDPR) replaces the UK's Data Protection Act 1998 (DPA) and will turn out to be part of UK law. The United Kingdom's Data Protection Act 2018 introduces a new public interest test applicable to the research processing of personal health data. The General Data Protection Regulation (GDPR), which comes into effect, will modernize and overhaul the legal framework for privacy and personal data protection across the EU. At the core of GDPR are seven fundamental principles – they're laid out in Article 5 of the legislation – which has been designed to guide how people's data can be handled. They don't act as hard rules but instead as an overarching framework that is designed to layout the broad purposes of GDPR.GDPR's seven principles are lawfulness, fairness, transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality (security); and accountability.

World Trade Organization's "***Telemedicine Agreement***" hypothesizes that "*In order for the WTO to serve as the body that facilitates international telemedicine, its members must commit to two key elements of the agreement. First, they must provide market access for the provision of telecommunications services. Second, they must provide market access for the*

[44] [2000] 1 All ER 786.
[45] 564 U.S. 552, 131 S. Ct. 2653 (2011).
[46] Application No. 20511/03: 2008 ECHR 623.
[47] Nimisha Srinivas, Arpita Biswas, *Protecting Patient Information in India: Data Privacy Law and Its Challenges* (2012) 5 NUJS L. REV. 411.

provision of medical services[48]."United Nations and its member states can support each other by providing the relevant technologies, bilateral plus multilateral agreement, and increase the use of telehealth technologies in this situation in order to exclude various factors.

V. CONCLUSION:

Undoubtedly, telemedicine is exceptionally beneficial for India absolutely; lawmakers just have to contemplate formulating the blue print for monitoring and regulating the said process. In order to gain patient's trust where 30% of the population is illiterate, we need strict laws for the privacy of the information of the patient and their data. Data privacy is crucial in India, which is governed by the Information technology act, 2000. Cybercrime is well mentioned in the legislation, but the execution part is not up to the mark because of less awareness. Many times, people who suffer due to a breach of data privacy didn't even want to register the complaint. Awareness and willingness to stop this kind of practice are an essential aspect of the company's growth.

COVID-19 pandemic leads to many difficulties not only to the economy but also to the health sector; because of this unseen virus, nobody is ready to contact one another because everybody is afraid of suffering from this deadly disease, it changed the everyday life and routine a lot. Now telehealth is giving way forward to keep track of the health sector smoothly. Telemedicine can not only solve this issue, but the distance and time factor can also be eliminated by looking at the geographical situation plus the health infrastructure in the cities in India.

Therefore, these extremities should be considered while formulating the policies as India doesn't have any specific legislation until now, and in 2020 modification has been witnessed only through the guidelines which were being issued by the government. Still, there is a long way to go. No doubt this pandemic has taught us many lessons, and the boost got up in the digital transaction.

[48] Kelly Cameron, *Facilitating International Telemedicine: The Way Forward* (1998), 23 INT'l LEGAL PRAC. 93.

REVIEWING THE LEGAL CONSIDERATIONS OF ARTIFICIAL INTELLIGENCE IN INDIA

Tabasum Ara[1]

ABSTRACT

Technology is changing our surroundings with increasing rapidity. New technologies are being incorporated more and more into our daily lives. Computer programs, algorithms and robots are replacing simple human activities. Amid these, Artificial Intelligence (AI) lies on the cutting edge of the technological spectrum in the world today. AI is the ability of a piece of equipment to imitate intelligent human behaviour. AI is a science and a set of computational technologies that are inspired by the ways people use their nervous systems to sense, discover, rationale, and take action. Artificial intelligence is that technology which has gradually penetrated in every aspect of our society, from the vital to the regular life. However, there is an apprehension of unforeseen misuse of this new technology which could be dangerous if not regulated. Presently, there are no explicit laws in India relating to AI. When we look at the adoption of artificial intelligence in India from a legal and regulatory point of view, the main issue we need to consider is are the existing laws sufficient to address the legal issues which might arise or do we need a new set of laws to regulate the artificial intelligence technologies? Whilst certain aspects like intellectual property rights and use of data to develop artificial intelligence might be covered under the existing laws, there are some legal issues which might need a new set of regulation to overlook the artificial intelligence technology. In this paper the researcher try to present an in-depth analysis of the legal challenges posed for AI systems. This paper attempts to highlight a few of such legal issues plaguing the AI industry and identify the key considerations for the technology. The researcher has made the use of secondary sources while reviewing the concept of Artificial Intelligence.

Introduction

The embracing and infiltration of Artificial Intelligence in our daily lives does not necessitate any more enunciation or illustration. While the technology is still considered to be in its infancy by many, its presence has been so intense that we do not comprehend our dependence on it unless it is specifically pointed out. From Siri, Google, Alexa to Amazon and Netflix, there

[1] **Phd Scholar, Department of Law, Central University of Kashmir**

is hardly any sector that has remained untouched by Artificial Intelligence. Thus, the adoption of artificial intelligence is not the challenge but its 'regulation' is a slippery slope which leads us to questions such as whether we need to regulate artificial intelligence at all? If yes, do we need a separate regulatory framework or are the existing laws enough to regulate artificial intelligence technology?[2]

The word "Artificial Intelligence" was coined by John McCarthy in 1956 and defined it as the science and engineering of making intelligent machines. AI is a swiftly advancing field of computer science. Theoretically, AI is the capability of a machine to recognize and react to its surroundings autonomously and perform tasks that would naturally require human intelligence and decision making processes, but without direct human intervention.[3] AI technology is mostly powered by Machine Learning and done by Deep Learning. It is also called computer intelligence or machine intelligence. This is the intelligence demonstrated by the machines. It is in contrast to natural intelligence displayed by humans and animals. If machines can perform the functions which are performed by humans and animals, it is called artificial intelligence. The data analytics attribute of AI which allows it to learn from its own experience allows it to have a deep learning process as such with natural language. It enables the computer machinery to perform the task solely which would have otherwise ordinarily required human intelligence. It also manages the learning from past experience to modify and avoid any ambiguity in future, thereby providing the machines a mind of their own to deal with situations. The reason for its necessity is the massive data-based services which are prevalent in every industry.[4]

Artificial Intelligence in India

Artificial Intelligence (AI) is hovering to disturb our world. AI presents opportunities to harmonize and enhance human intelligence and improve the way people subsist and work. India, being the quickest developing economy with the second biggest populace on the planet, has a huge stake in the AI transformation. The intelligent machines are now empowering high-level

[2] Pramit Bhattacharya. [2020]. Core Legal Issues with Artificial Intelligence in India. <https://www.foxmandal.in/core-legal-issues-with-artificial-intelligence-in-india> accessed 15 January 2021

[3] Rigano, C. (2019). Using Artificial Intelligence to Address Criminal Justice Needs. *NIJ Journal*, Issue 280.

[4] Pragya Rao & Rakesh Fartyal, 'Artificial Intelligence and Indian Legal System: An Analysis' [2020] 2 (6) FastForward Justice's Law Journal

intellectual processes like thinking, perceiving, learning, critical thinking, combined with advances in information compilation and aggregation, analytics and computer processing power.[5] In India, there has been an important growth in interest levels around AI across all industry sectors. Although AI consideration is significantly smaller in India than in USA or China , the increased AI interest has been reflected in the following three ways:

1. Industries have begun working to empower and improvise the skill of their manpower in order to compete with other countries.
2. Educational institutions have started incorporating the courses on machine learning in their institutional curricula.

3. Individuals and professionals have started acquiring these skills and are investing in advancement of their own skills.

There are many instances in India where AI has been widely used and it resulted to be productive. Lately, the police of Kerala initiated a robot for police work. The first humanoid police robot of Sub Inspector (SI) rank in India, was introduced in Thiruvananthapuram of Kerala. The robot performs the duties of the front office of police headquarters. It receives the visitors & directs them to different places according to their needs.[6] Similarly, Chennai got its second robot-themed restaurant where the robotic waiters serve the food. These robots interact with customers in both English and Tamil. The restaurant is situated in Chennai's Mugilivakkam-Porur, and has a team of seven robots. They offer a temperate greeting to the customers and bring meals and exotic drinks to their table. A female robot at the reception gives a response to customers' queries and guides the customers about their table numbers. They have two types of robots, one for serving food and the other one to interact and guide the customers.[7] In Ahmedabad, Gujarat a cardiologist performed the world's first in-human telerobotic coronary intervention on a patient nearly 32 km away. This was an important breakthrough in medical science was achieved in Gujarat on Wednesday when cardiac surgeon performed Tele-robotic

[5] NITI AAYOG, 'Discussion Paper National Strategy for Artificial Intelligence' [2018]

[6] <https://www.thehindubusinessline.com/news/national/kerala-police-introduces-countrys-first-humanoid-robot-into force/article26318193.ece#:~:text=As%20a%20police%20force%20that,%2DBot%2C'%20Abraham%20said> accessed 12 January 2021

[7] < https://www.indiatoday.in/india/story/in-this-chennai-restaurant-robot-waiters-serve-customers-speak-to-them-in-tamil-and-english-1449122-2019-02-06> accessed 12 January 2021

surgery from a remote location using robotically controlled instruments. The patient was a middle-aged woman with a blocked artery.[8] All these examples represent the arrival of Artificial Intelligence (AI) in everyday lives of human beings even in India.

India may become the capital of artificial intelligence (AI) because of the talent of its people. However, this development can be accelerated by a policy framework.[9] The budding technologies such as artificial intelligence (AI) have compelled us to re-imagine our businesses and make them more lively, elastic and approachable. While the whole world is battling the pandemic of coronavirus, the need of the hour is to put the focus firmly on AI and the way it will redefine the reality of the post-Covid world. Artificial Intelligence (AI) could potentially add to India's gross domestic product (GDP) and drive India's economic growth.

But at this point of time, there have been no regulations or adjudications by the Courts acknowledging the legal status of artificial intelligence. Defining the legal status of AI machines would be the first cogent step in the framing of laws governing artificial intelligence and might even help with the application of existing laws. A pertinent step in the direction of having a structured framework was taken by the Ministry of Industry and commerce when they set up an 18 member task force in 2017 to highlight and address the concerns and challenges in the adoption of artificial intelligence and facilitate the growth of such technology in India. The Task Force drafted a report in March 2018 [10], in which they provided recommendations for the steps to be taken in the formulation of a policy. The Report identified ten sectors which have the greatest potential to benefit from the adoption of artificial intelligence and also cater to the development of artificial intelligence-based technologies. The report also highlighted the major challenges which the implementation of artificial intelligence might face when done on large scale, namely " (i) Encouraging data collection, archiving and availability with adequate safeguards, possibly via data marketplaces/exchanges; (ii) Ensuring data security, protection, privacy and ethical via regulatory and technological frameworks; (iii) Digitization of systems

[8] <http://www.hcghospitals.in/SpecialitiesDetail/hcg-cancer-centre-ahmedabad/robotic-surgery/1/43> accessed13 January 2021

[9] Chandrasekaran, N. Tata Sons Chairman

[10] Ministry of Commerce and Industry, Government of India., 'The Report of The Artificial Intelligence Task Force'[2018] https://dipp.gov.in/sites/default/files/Report_of_Task_Force_on_ArtificialIntelligence_20March2018_2.pdf> accessed 15 January 2021

and processes with IoT systems whilst providing adequate protection from cyber-attacks; and (iv) Deployment of autonomous products and mitigation of impact on employment and safety".[11]

The Task Force also recommended establishment up of an **'Inter–Ministerial National Artificial Intelligence Mission',** for a period of 5 years, with financial support of around 1200 Crores, to act as a nodal agency to coordinate all AI-related activities in India.
The Budget of 2019 also proposed to initiate a national programme on AI. But all these developments are taking place on the technological front. No inclusive legislation to regulate this mounting industry has been formulated in India till date.

Some Legal Issues of AI

When we look at the adoption of artificial intelligence from a legal and regulatory point of view, the main issue we need to consider is, are the existing laws sufficient to address the legal issues which might arise or do we need a new set of laws to regulate the artificial intelligence technologies. Whilst certain aspects like intellectual property rights and use of data to develop artificial intelligence might be covered under the existing laws, there are some legal issues which might need a new set of regulation to overlook the artificial intelligence technology.

1. Liability of Artificial Intelligence

The current legal regime does not have a framework where a robot or an artificial intelligence program might be held liable or accountable in case a third party suffers any damage due to any act or omission by the program. For instance, let us consider a situation where a self-driven car controlled via an artificial intelligence program gets into an accident. How will the liability be apportioned in such a scenario? The more complex the artificial intelligence program, the harder it will be to apply simple rules of liability on them. The issue of apportionment of liability will also arise when the cause of harm cannot be traced back to any human element, or where any act or omission by the artificial intelligence technology which has caused damage could have been avoided by human intervention. One more instance where the current legal regime may not be able to help is where the artificial intelligence enters into a contractual obligation after negotiating the terms and conditions of the contract and subsequently there is a

[11] Ibid.

breach of contract.[12] The pertinent legal question here is what kind of rules, regulations and laws will govern these situations and who is to decide it, where the fact is that artificial intelligence entities are not yet considered to be subject of law.

2. Status of Artificial Intelligence Entities

From a legal point of view, personality of an entity is an extremely important factor to assign rights and obligations. Personhood can either be natural or legal. Attribution of personality is important from the point of view that it would help identify as to who would ultimately bear the consequences of an act or omission. Artificial intelligence entities, to have any rights or obligations should be assigned personhood to avoid any legal loopholes. **'Electronic personhood'**[13] could be attributed to such entities in situations where they interact independently with third parties and take autonomous decisions. Therefore, it is indispensable to set up the legal personality of AI which means AI will have a collection of privileges and obligations, in the context of India's criminal law jurisprudence.

3. Protection of Privacy and Data

For the development of better artificial intelligence technologies, the free flow of data is crucial as it is the main fuel on which these technologies run. Thus, artificial intelligence technologies must be developed in such a way that they comply with the existing laws of privacy, confidentiality, anonymity and other data protection framework in place. There must be regulations which ensure that there is no misuse of personal data or security breach. There ought to be instruments that enable users to stop processing their personal data and to invoke the right to be forgotten.[14] It is further to be seen whether the current data protection/security obligations should be imposed on AI and other similar automated decision-making entities to preserve individual's right to privacy which was declared as a fundamental right by the Hon'ble Supreme Court in Justice **K. S Puttaswamy & Anr. v Union of India and Ors**[15]. This also calls for an

[12]Pramit Bhattacharya, 'Core Legal Issues with Artificial Intelligence in India' [2020] https://www.foxmandal.in/core-legal-issues-with-artificial-intelligence-in-india/ > accessed 15 January 2021

[13] James Vincent, 'Giving robots 'personhood' is actually about making corporations accountable'(The Verge 19 January 2017) <https://www.theverge.com/2017/1/19/14322334/robot-electronic-persons-eu-report-liability-civil-suits> accessed 15 January 2021

[14] Pramit Bhattacharya, 'Core Legal Issues with Artificial Intelligence in India'[2020] <https://www.foxmandal.in/core-legal-issues-with-artificial-intelligence-in-india/> accessed 15 January 2021

[15] Writ Petition (Civil) No 494 of 2012 Decided in 2018

all-inclusive data privacy regime which would apply to both private and public sector and would govern the protection of data, including data used in developing artificial intelligence. Similarly, surveillance laws also would need a revisiting for circumstances which include the use of fingerprints or facial recognition through artificial intelligence and machine learning technologies.

At this point in time there are a lot of loose ends to be tied up like the rights and responsibilities of the person who controls the data for developing artificial intelligence or the rights of the data subjects whose data is being used to develop such technologies. The double-edged sword situation between development of artificial intelligence and the access of data for further additional purposes also needs to be deliberated upon.

4. Protection of Ownership

It is hardly impossible to think about the application of AI without any legal implications. It is difficult to comprehend the categorisation of AI under copyright law and/or patent law. Is AI a mere tool and therefore the owner of the tool should be identified with the intellectual property generated by such tool or should the AI application itself be recognised as the owner of intellectual property? These issues constantly crop up as regarding the protection of ownership of AI applications. Therefore the existing laws of India need to be reviewed to keep up with the advancement in field of AI and its diverse applications till a special law is framed exclusively for AI applications.

Concluding Remarks

The rate of adoption of AI and related technologies continues unabated with extensive, worldwide, and rapid acceptance. Adoption of AI by organizations continues to grow up. However, with this growth of adoption there comes strain as existing regulation and laws struggle to deal with emerging challenges of this technology. As a result, the world governments are constantly working to ensure that existing laws, regulations, and legal framework remain relevant in the face of technology change and can deal with new, emerging challenges posed by AI. It is not unforeseen to find that most governments like India are adopting a 'wait and see'

approach in respect of laws and regulations on AI. "Just like with any new technological wave it's hard to predict just how this new technology will be used, or abused. It took many years before laws were put in place to regulate the use of cell phones while driving". This is due to the reason that lawmakers needed to see how the technology was being used, the involved hazards, and only then they would able to come up with meaningful laws to regulate the use of the technology.[16] Same is the case with AI. It's still too early for government to see how this technology will impact citizens. At global level, the countries like india too are active in proposing new rules and regulations, with existing or proposed rules. AI need to be regulated in a proper manner if not regulated it can have unmanageable issues. India should be ready to face this destructive technology.

While the moral and responsible use of AI continues to be an important topic for discussion, no country has advanced any precise legislation or regulation with regard to the ethical use of AI or any issues regarding prejudice in the application or development of AI systems. The United Kingdom, European Union, Australia, Singapore and Germany are all vigorously taking into consideration such regulation and have advanced discussions around this topic. However, no country has yet put any specific law in place around ethical and responsible role of AI. It is to be seen whether or not companies will self-monitor or if governments will step in to regulate more formally. And, with regard to intentional malicious use of AI, there is also no legislative or regulatory activity. We expect to see more discussion and regulation around this issue,once some big incident comes to the surface. Adoption for AI shows no signs of slowing and governments are paying attention. So AI laws are coming.[17]

AI systems have the potential to learn from experience and to perform unconventionally for humans. This also makes AI the most troublesome and self-transformative technology of the 21st century. So, if AI is not regulated properly, it is bound to have insurmountable implications. e.g. the outcome is unimaginable, if electricity supply stops suddenly while a robot is performing a surgery and access to a doctor is lost. These questions have been already confronted by courts in the U.S. and Germany. All countries, including India, need to be legally prepared to face such kind of disorderly technology. The first step to be taken is to have a legal definition of AI in

[16] Kathleen Walch, 'AI Laws are coming'[2020] <https://www.forbes.com/sites/cognitiveworld/2020/02/20/ai-laws-are-coming> accessed 15 January 2021
[17] Ibid.

place. Since AI is considered to be inorganic, a liability scheme that will hold the producer or manufacturer of the product liable for harm must be carefully taken into consideration. Moreover, since privacy is a fundamental right, certain rules to regulate the usage of data possessed by an AI entity should be framed. This should be a part of the Personal Data Protection Bill, 2018 also.[18]

[18] Need for a Legal Framework for AI in India. https://www.iasparliament.com/blogs/pdf/need-for-a-legal-framework-for-ai-in-india

LEGAL ISSUES UNDER ARTIFICIAL INTELLIGENCE

Sivarama Krishna Prakash [1]

Abstract

AI is broadly described as either: narrow AI (also referred to as "weak" or applied AI), which carries out a function such as data processing; or artificial general intelligence (AGI or "strong" AI), which is hypothetically capable of "the whole domain of human thought." Artificial general intelligence that surpasses "the best human brains in practically every field" would be considered artificial superintelligence (ASI). Present day AIs are mostly narrow AI and they are generally built to solve particular tasks. Development of AGI is very rare and generally unheard of. However, there is a fair possibility of companies researching on AGI in stealth mode. AI permeates our lives in numerous subtle and not-so-subtle ways, performing tasks that, until quite recently, could only be performed by a human with specialized knowledge, expensive training, or a government-issued license. Driverless cars, which also are propelled by AI, have been approved for road operation in four states of the United States of America and the District of Columbia; their inevitable arrival on the consumer market is expected to revolutionize road transportation. Autonomous machines have the capability to execute complex financial transactions, flag potential terrorists using facial recognition software, and perform document review.

The ***core issues*** arising out of usage of AI are Legal status of AI and liability for accidents caused by AI machines. Legal personhood is inherently linked to individual autonomy. No law currently in force recognises AI as a legal person. However, with Sophia, a humanoid being granted citizenship by Saudi Arabia, coupled with the recent accident caused by Uber's self-driving car, it has become imperative to address the legal personhood of AI. The question of whether legal personhood can be conferred on an AI boils down to whether it can be made the subject of legal rights and duties. Another issue that arises is attributing liability to an AI. As on date no law qualifies AI as a legal person and hence it cannot be held liable in its own capacity. The biggest roadblock to reconsider this rule is the conundrum as to how to penalise an AI for its wrongdoing, which has not been dealt with as of today. As an example, if we take the case of

[1] Ph.D Scholar, Alliance University

accident caused by an autonomous vehicle, there are multiple persons who could be responsible e.g. the Maker of the AI, Developer, Quality Control team, User, person responsible to provide software updates, malware patches etc. This paper will delve more deeper into all the above.

1. Introduction

Artificial Intelligence or AI is broadly described as either: narrow AI (also referred to as "weak" or applied AI), which carries out a function such as data processing; or artificial general intelligence (AGI or "strong" AI), which is hypothetically capable of "the whole domain of human thought." Artificial general intelligence that surpasses "the best human brains in practically every field" would be considered artificial superintelligence (ASI). Present day AIs are mostly narrow AI and they are generally built to solve particular tasks. Development of AGI is very rare and generally unheard of. However, there is a fair possibility of companies researching on AGI in stealth mode.

AI permeates our lives in numerous subtle and not-so-subtle ways, performing tasks that, until quite recently, could only be performed by a human with specialized knowledge, expensive training, or a government-issued license. Driverless cars, which are also propelled by AI, have been approved for road operation in four states of the United States of America and the District of Columbia; their inevitable arrival on the consumer market is expected to revolutionize road transportation. Autonomous machines have the capability to execute complex financial transactions, flag potential terrorists using facial recognition software, and perform document review.

Present day AI is no longer a fiction. It is more of science, with computers and robots replacing humans. AI basically is the capability of a machine to imitate intelligent human behaviour. With the advent of new technologies, the influx of AI in our day-to-day lives is slowly becoming inevitable.

2. **Core Issues.** The core issues arising out of usage of AI are as follows:
   a. **Legal Status of AI.** Legal personhood is inherently linked to individual autonomy. No law currently in force recognises AI as a legal person. However, with Sophia, a humanoid

being granted citizenship by Saudi Arabia, coupled with the recent accident caused by Uber's self-driving car, it has become imperative to address the legal personhood of AI. The question of whether legal personhood can be conferred on an AI boils down to whether it can be made the subject of legal rights and duties. The legal fiction created for corporates serves as a precedent for granting legal personhood to AI. However, there exists a distinction between corporates and AI.[2] Corporates are fictitious persons who are accountable via their stakeholders. As against this an AI may be actually independent. As a centre path one could possibly grant AI a bundle of rights selected from those currently ascribed to legal persons.

b. Liability on account of wrong actions or accidents caused by AI. Another issue that arises is attributing liability to an AI. As on date no law qualifies AI as a legal person and hence it cannot be held liable in its own capacity.[3] The biggest roadblock to reconsider this rule is the conundrum as to how to penalise an AI for its wrongdoing, which has not been dealt with as of today. As an example, if we take the case of accident caused by an autonomous vehicle, there are multiple persons who could be responsible e.g. the Maker of the AI, Developer, Quality Control team, User, person responsible to provide software updates, malware patches etc.

3. Other Issues. Some of the other issues that arise with use of AI are as follows:

a. Contractual relationships. Another issue is the ability of an AI to execute and be bound by contracts. Under Indian law only a "legal person" can be competent to enter a valid contract. The general rule thus far has been that an AI may not qualify as a legal person. Hence, a contract entered into by an AI of its own volition may not be regarded as a valid contract in India. Resultantly, steps need to be taken to ensure that

[2] Tavawalla H and Senthilnathan A, "Can Artificial Intelligence Be given Legal Rights and Duties?" (*Lexology*J une 19, 2018) <https://www.lexology.com/library/detail.aspx?g=15937d6a-5421-487b-bf60-82a34cb79d79> accessed January 9, 2020

[3] Tavawalla H, "India: Can Artificial Intelligence Be Given Legal Rights And Duties?" (*Can Artificial Intelligence Be Given Legal Rights And Duties? - New Technology – India* June 25, 2018) <http://www.mondaq.com/india/x/712308/new technology/Can Artificial Intelligence Be Given Legal Rights And Duties?sa=X&ved=2ahUKEwjLvemP9fXmAhVQH7kGHaU6AfIQFjACegQIBhAB> accessed January 9, 2020

technology standards are developed to adequately regulate contracts entered into by AI.[4]

b. Employment and AI. Demand and need for automation catapulted the development of AI. With the objective of increasing efficiency, companies across the world have prescribed to the practice of utilizing AI as a replacement of the human workforce. Growing use of AI in workplace due automation is creating a gap in the existing employment laws. Some of the prominent issues that could arise when using AI for employment could be:

i. Provident Fund and Gratuity eligibility for AI,
ii. Rights of AI to sue a company for wrongful termination of employment.

AI requires individuals to function. Hence employment laws need to have more clarity on human and AI liability especially when AI is handled by individuals as absence of such laws may adversely impact such individuals, as well.

c. **Regulation of AI.** With the passage of time influx of self-driven cars, robots and fully automated machines is only expected to increase. As a result, the dependency of society as a whole on AI systems is also expected to rise. To safeguard the integration of AI, a balanced approach would need to be adopted which efficiently regulates the functioning of AI systems but also maximises its benefits. International standardisation is also very much essential.

d. **Reducing human status.** Humans aren't the only people in society – at least according to the law. In the U.S., corporations have been given rights of free speech and religion. Similarly, people argue that an artificial intelligence system can also be recognized as a person – without any legislation, court rulings or other revisions to existing law. However, by doing so there is a fair possibility that human rights and dignity would suffer as a result. For instance, when Saudi Arabia granted citizenship to a robot called Sophia, human women, including feminist scholars,

[4] Ibid 1.

objected, noting that the robot was given more rights than many Saudi women have. In certain places, some people might have fewer rights than nonintelligent software and robots. In countries that limit citizens' rights to free speech, free religious practice and expression of sexuality, corporations – potentially including AI-run companies – could have more rights. That would be an enormous indignity. The risk doesn't end there: If AI systems became more intelligent than people, humans could be relegated to an inferior role – as workers hired and fired by AI corporate overlords – or even challenged for social dominance.[5]

e.

Artificial intelligence systems could be tasked with law enforcement among human populations – acting as judges, jurors, jailers and even executioners. Warrior robots could similarly be assigned to the military and given power to decide on targets and acceptable collateral damage – even in violation of international humanitarian laws. Most legal systems are not set up to punish robots or otherwise hold them accountable for wrongdoing.[6]

f. **Voting.** Granting voting rights to systems that can copy themselves would render humans' votes meaningless. Even without taking that significant step, though, the possibility of AI-controlled corporations with basic human rights poses serious dangers. No current laws would prevent a malevolent AI from operating a corporation that worked to subjugate or exterminate humanity through legal means and political influence. Computer-controlled companies could turn out to be less responsive to public opinion or protests than human-run firms are.

g. **Immortal wealth.** Two other aspects of corporations make people even more vulnerable to AI systems with human legal rights: They don't die, and they can give unlimited amounts of money to political candidates and groups. Artificial intelligences could earn money by exploiting workers, using algorithms to price

[5] Longmont Observer Staff, "Could An Artificial Intelligence Be Considered A Person Under The Law?" (*Longmont Observer* October 9, 2018) <https://longmontobserver.org/lifestyle/could-an-artificial-intelligence-be-considered-a-person-under-the-law/> accessed January 9, 2020

[6] Yampolskiy RV, "Could an Artificial Intelligence Be Considered a Person under the Law?" (*Phys.org* October 5, 2018) <https://phys.org/news/2018-10-artificial-intelligence-person-law.html> accessed January 9, 2020

goods and manage investments, and find new ways to automate key business processes. Over long periods of time, that could add up to enormous earnings – which would never be split up among descendants. That wealth could easily be converted into political power.[7]

h. **Unethical Practices.** Politicians financially backed by algorithmic entities would be able to take on legislative bodies, impeach presidents and help to get figureheads appointed to the Supreme Court. Those human figureheads could be used to expand corporate rights or even establish new rights specific to artificial intelligence systems – expanding the threats to humanity even more.

i.

4. Existing Legal Situation

Litigation for accidents or incidents caused during usage of AI will definitely be complicated even though the legal basis for professional liability would more or less be the same as in the case of non-AI involved accidents. As regards AI persons, there are no predefined AI specific legal frameworks to affix culpability & liability and determine valid and effective sentence. As an example if we look at accidents or incidents caused during Robot assisted surgeries, in addition to physician and hospital, the manufacturer of the robotic system and third-party individual (in cases of hacking) may be sued. The existing process is to fall back on present laws for both civil and criminal liability and prove the blameworthiness/guilt of each of the actor and then assess the culpability, liability and punishment.

Criminal Act is one of the basic requirements to sustain criminal liability and imposing a punishment. Criminal Act is something which can only be done by humans or attributed to humans. To fix culpability for a crime done by an AI, we should be able to pinpoint human(s) who can be made liable for criminal liability, i.e they should have done the criminal act or actus reus[8] and should have a guilty mind or mens rea[9], to whom the crime can be attributed. In order

[7] Yampolskiy RV, "Could An Artificial Intelligence Be Considered A Person Under The Law?" (*International Business Times* October 9, 2018) <https://www.ibtimes.com/could-artificial-intelligence-be-considered-person-under-law-2723274> accessed January 9, 2020

[8] A Dictionary of Law (8th edn, 2015) 15.
[9] ibid 395-96.

to fix attributability to a person for having done a criminal act there would be a necessity to identify the persons involved in the AI and its decision making.[10] Some of the actors are:

a. The first person who can be identified is the user.[11] The user is normally a person who uses and controls the AI in its operations and provides instructions to the AI about the various tasks that it has to do. The user in all probabilities would be the first beneficiary of the work done by the AI. Going by past precedence, it can be clearly concluded that the general tendency is that the user and supervisor have mostly been the persons who have been involved in criminal investigations looking into the behaviour of an AI.

b. The second person in the chain would be the supervisor, who has the responsibility to supervise the AI and has the right controls or opportunity to intervene in the decision-making of the AI, if necessary.

c. The third person in the chain would be the producer or manufacture of the AI as they are generally responsible for anything and everything that concerns the production of the AI, including but not limited to hardware, software and other utility related features. The producer has in-depth knowledge of the backend technology or platform under which the decision-making process in the AI runs. The producer also has the capacity and wherewithal to rise or fall to the expectation levels of the other actors especially with respect to the capability of the AI.[12]

d. In most of the cases the producer may not necessarily be the software coder and this task would have been outsourced to a third party. Such third-party software coders or developers would also generally fall in the category of producer, despite the fact that the software coder would actually be a third party to whom the producer would have outsourced the coding work.

[10] Simester AP and others, *Criminal Law: Theory and Doctrine* (Hart Publishing 2016) 72.
[11] Weaver JF, *Robots Are People Too: How Siri, Google Car, and Artificial Intelligence Will Force Us to Change Our Laws* (Praeger 2014) 3.

[12] Daniel C Vladeck, *'Machines Without Principals: Liability Rules and Artificial Intelligence'* (2014) 89

e. Before the sale of the AI or machine the owner would generally be the producer. After the sale, the owner in all likelihood would be either the user or the supervisor. However, indicating the ownership of the AI is very important as that role will be important for any future analysis especially if there is a change in law from the time of manufacture to the time of offence (de lege ferenda).

f. The last actor possibly is a third party who is an outsider and has no relationship with the AI. However, this third party has the ability and capacity to interact with the AI and affect or alter its behaviour. Such a third party could possibly be a human who could possibly be a hacker or someone performing similar tasks, or in case of non-humans, a malware or virus.

Impact and ability are generally the main factors to determine criminal liability as well as responsibility with respect to matters leading to the factors causing the consequences of the crime. As regards liability for crimes committed by AI, we need to trace an AI's criminal act and behaviour to the human(s) behind the AI as it is fairly clear that under the existing legal regime an AI is not legally accountable for its conduct. The human on whom such culpability is intended to be fixed must have the position and capability to influence the AI and its conduct in some way. Consideration of factors in this analysis will vary from case to case. Notwithstanding the above, one cannot overlook the fact that the responsibilities of the supervisor and user would also have a direct connection with the use of the AI. The various actors as described above may have a role to play in controlling the AI either remotely through their instructions or by omitting to provide requisite instructions to override the AI where required. AI users can remotely control any AI machine or Robot controlled by AI and intentionally cause harm to the AI user.

To solve this example and attribute liability is not a difficult proposition so long as one considers the Robot as a tool used to injure a human being. However, the question of liability becomes complicated as soon as the Robot ignores the instructions given to it by the user and acts autonomously causing serious damage. One of the primary questions that would arise is if

there is a duty cast on the user or supervisor to abrogate such behaviour by the Robot and do, they have the capacity and control to override the Robot's actions? When it comes to the producer's responsibility or liability, most of it can generally be linked to the AI software and/or hardware with associated algorithms, mechanical parts and movements of the AI and also the AI's education and training.[13] It is also evident that the producer has a vast scope to influence the AI in any area. The software code in an AI can also be called the AI's brain and that is the core factor and the key to an AI's capability.[14] Any malfunction pointing to a production issue will in all probabilities be traced back to the producer and its sub-contractors. However, there could be situations where the AI causes wrongs which were not foreseen by the producers while manufacturing or by the coder when they wrote the software code. In such cases there are two things that will come to the forefront during investigation. One is if the producer provided overriding controls to the AI user. The next is if the AI user or supervisor are responsible in the scheme of things to abrogate such wrong actions by the AI. In any investigation regarding a wrong act committed by an AI, the owner will definitely be one of the key indispensable actors who would be questioned in depth to determine and affix the liability.

As mentioned above there will also be outsiders who can or would have influenced the AI in its decision-making, who would be more or less self-evident in criminal liability case. Such outsiders could be a remote-control hacker or a third party who controls the intelligence of an AI by presenting an idea. There could also be outsiders who can fool the AI to misunderstand its environment in such a way, resulting in wrongdoing by the AI.

5. Ethical Issues when using AI.

Ethical issues during usage of AI are also of paramount importance and one must be mindful of equipment safety and reliability, provision of adequate information, and maintenance of

[13] Cindy M Grimm, William D Smart and Woodrow Hartzog, *An Education Theory of Fault for Autonomous Systems*, (WeRobot 2017 conference, New Haven, Mars 2017) <www.werobot2017.com/wp-content/uploads/2017/03/Smart-Grimm-Hartzog-Education-We-Robot.pdf> accessed 02 Feb 2020.
[14] Nick Bostrom, *Superintelligence: Paths, Dangers, Strategies* (OUP 2014) 23

confidentiality. The following are some key ethical and societal issues that are of concern when using AI:[15]

a. **Security & Privacy.** Data security is a primary concern for a connected system. Historic information and any additional current relevant information of the patient and the surrounding world is a mandatory requirement for an AI system to help it adapt to the user's changing needs and circumstances. The above information can be clearly categorised as sensitive information, which if shared inappropriately could compromise the individual's dignity and right to privacy.

b. **Transparency**. The users must clearly know what an AI system does and what it cannot do. The users must understand why an AI system is performing a task at a specific location/time, what kind of data is being collected by the AI system and if such collected data is being shared. The AI system must be able to give an account of what it is doing and thereby enable users to understand and speedily respond to situations on as required basis.

c. **Social Attachment.** Humans already have emotional bonds their mobile phones, tablets and cars. Over a period of time, they would develop similar bonding with AI technologies including companion robots. Hence the AI designer must definitely give careful consideration while designing to ensure that machines and humans don't entangle their relationships.

d. **Autonomy of Decision Making.** As the AI systems become more complex, the expectations will increase. Matured machines will be expected to make more demanding decisions in course of their work. The Intelligent AI machines as they mature will at times have to reason internally and arrive at their own best conclusions. The AI manufacturers have to ensure that these machines do not operate outside the laid down

[15] Consequential Robotics, "8 Ethical and Societal Issues Relevant to the Future Use of Robots in Social Care" (*Consequential Robotics*, March 12, 2018) <http://consequentialrobotics.com/blog/2018/3/12/8-ethical-and-societal-issues-relevant-to-the-use-of-robotics-autonomous-systems-in-social-care> accessed February 2, 2020

parameters and if they do so either the machine must automatically stop or if user operated then the user must be able to take control.

e. **Impact on Caretakers.** AI is something which is there to stay and will definitely impact on future social care delivery. However, AI may not end up substituting humans in the care sector. AI can be developed to supplement human care activities, but they are not likely to match or replace the ability of humans in the near future as humans have empathy and can provide an engaging relationship which cannot be replaced by the synthetic companionship provided by AI.

f. **Governance.** Great amount of efforts is underway to develop governance frameworks for AI and robotics. United Kingdom is considering governance of data, and hence have set up a Commission on the moral and societal impacts of AI. Governance and regulatory policies and mechanisms must be internationally standard and also recognised by most nations of the world for it to be effective.

6. Sentencing for Criminal Acts committed by Robots/AI Persons.

Robots are slowly becoming a part and parcel of our lives and we are slowly trusting them. However, it has been seen that in some cases the results have been catastrophic:

a. Robots that are used for medical practices have been injuring and killing its patients.
b. In 1979 a robot killed a human in a Ford Motor Company plant. The next death was in 2015 in a German factory and in 2017 another human died due to a robot in Michigan.
c. The famous Tesla autonomous car accident occurred in May 2016 wherein the car collided with a tractor-trailer and killed the Tesla driver.
d. In March 2018, an Uber self-driving car in Arizona hit and killed a pedestrian.

In the United States a study was carried out regarding the safety of surgical robots. It surfaced that Robots had caused 144 deaths and more than 1,000 injuries over a 14-year period. Some of these accidents included injuries to patients' bodies through broken instruments. The

other major injury was tissue burns through electrical sparks. Long delays in surgery due system errors were also a contributory factor for the deaths. The bottom line of the study was very clear about the need for fresh safety measures. The study also highlighted that a number of technical difficulties and complications are still being experienced during robot assisted medical procedures.[16] Formulation of clear-cut laws to handle AI related is still in nascent stage worldwide and most nations use a mix of conventional laws including law of torts to decide on AI related claims/cases.

7. Uber Self Driving Vehicle Crash in Tempe, Arizona – Case Study

a. **Case Summary.** On 18 March 2018, when Ms. Herzberg was crossing the road at Mill Avenue outside the designated pedestrian crosswalk, pushing a bicycle laden with shopping bags, she was stuck by a prototype Uber self-driving Volvo XC90 car. Ms. Herzberg died of injuries in the hospital. The investigations revealed that the speed of the vehicle required emergency braking system to work. Uber had disabled the factory settings for emergency braking to "reduce potential for erratic vehicle behaviour." As per Uber even though the car was on autonomous mode legally the on-board safety driver was supposed to take on control in case of such emergency, which did not happen. National Transportation Safety Board ("NTSB") did not apportion any blame to Uber in their preliminary report and mentioned that "All aspects of the self-driving system were operating normally at the time of the crash, and there were no faults or diagnostic messages" [17]. NTSB also mentioned that "the safety driver Ms. Rafaela Vasquez failed to intervene and hence the collision could not be prevented. Ms. Rafaela spent 34% of her time watching a TV show on her mobile and she just responded by moving the steering wheel less than a second before impact and engaged the brakes less than a second after impact."

b. **Video Footage Analysis.** The Tempe Police carried out an analysis of dashboard cameras and released two videos showing footage recorded by the two onboard

[16] "Robotic Surgery Linked to 144 Deaths in the US" (*BBC News,* July 22, 2015) <https://www.bbc.com/news/technology-33609495> accessed February 2, 2020

[17] "Uber-self-driving-crash-ntsb-report" <https://www.theverge.com/2018/5/24/17388696/uber-self-driving-crash-ntsb-report> accessed January 10, 2021

cameras: one forward-looking, and one capturing the safety driver's actions. The front facing camera indicated that the car was travelling in far-right lane when the collision took place. The driver-facing camera indicated that the safety driver was looking down before the collision. When questioned the driver defended and mentioned that she was monitoring the center stack at the time of the collision[18].

c. **Software Issues.** The vehicle software did have issues. The instrument recording or telemetry recording revealed that the victim was detected only six seconds prior to the crash. The victim was initially classified as an unknown object, then as a vehicle, and finally as a bicycle. The autonomy logic had different predicted paths for each of these three identities.

d. **Sensor issues.** The car was equipped with advanced sensors which included Radar and LiDAR sensors. These sensors are not normally affected by darkness and hence it was safely concluded that there were no sensor issues and if at all there was any issue it was the safety driver not taking control when required.

e. **Actions by Uber post the Accident.** Following the fatal incident, Uber suspended testing of self-driving vehicles in Arizona and thereafter restarted it nine months later. Uber chose not to renew its permit for testing self-driving vehicles in California, when it expired at the end of March 2018. In February 2020, the California Department of Motor Vehicles re-issued the permit afresh[19] to Uber Advanced Technologies for testing of Autonomous Vehicles and Uber thereafter has started testing in San Francisco. Uber in collaboration with Volvo has now come up with a third generation Autonomous Car which has a lot of redundancy, specifically around steering, braking, and battery power[20]. Uber has

[18] "NTSB Investigations" >https://www.ntsb.gov/investigations/AccidentReports/Reports/HWY18MH010-prelim.pdf> accessed January 10, 2021

[19] "Uber Gets Permit to Restart Testing its self-driving cars in California" https://www.reuters.com/article/us-uber-self-driving/uber-gets-permit-to-restart-testing-its-self-driving-cars-in-california-idUSKBN1ZZ2QG accessed on January 10, 2021

[20] "Uber-Volvo Self-Driving Car Safety" https://www.theverge.com/2019/6/12/18662626/uber-volvo-self-driving-car-safety-autonomous-factory-level accessed on January 10, 2021

mentioned that "If any of the primary systems should fail for some reason, the back-up system is designed to immediately act to bring the car to a stop." NTSB had in one of their reports blasted Uber for poor safety culture. Uber thereafter also stated that going forward it will not disable the automatic braking system.

f. **Current Status of the Case.** Post investigation NTSB split the blame between Uber, the safety driver, the victim (apart from crossing road at a non-designated place also had tested positive for methamphetamine and marijuana) and the State of Arizona. The NTSB report mentioned the failure of the federal government in properly regulating the Autonomous Vehicles industry. Uber was cleared of any criminal wrongdoing by local authorities. Uber settled a lawsuit with Herzberg's family for an undisclosed sum[21]. Ms Vasquez was charged on 27 August 2020 and made her first appearance in court on 15 September 2020. The trial is now expected to commence in February 2021.

g. **Issues having no clear answer in investigation so far.** Even though the names of Arizona State and Uber figured out in the initial investigations. No final charge sheet has been filed against them. The only case now pending in the court is that against the safety driver. Uber managed to close the case filed by the relatives of the deceased by compensating them for an undisclosed sum. Under normal circumstances one would have expected Uber and State of Arizona to have been made responsible under **Absolute Liability** doctrine (akin to the MC Mehta Bhopal gas case). Uber for negligence (jeopardizing public safety) by choosing to disable the lifesaving feature in such a technology which may endanger human lives and State of Arizona for not having proper clarity in the law/policy related to testing of Autonomous Vehicles. It is surprising that this did not happen. Also there seems to be no **Product Liability** case filed against Uber/Volvo/any one the software/sensor vendors of the AI systems used in the vehicle involved in the crash. That's the second surprise exclusion.

[21] "Uber Self Driving Car Resume Testing" https://www.theverge.com/2020/3/10/21172213/uber-self-driving-car-resume-testing-san-francisco-crash accessed on January 10, 2021

h.

8. **Conclusion.**

It is quite evident that when it comes to rules governing AI machines or systems, we definitely lack clarity. In the absence of clear-cut laws and regulations, what obligations and consequences apply to mishaps/accidents caused by AI systems are unknown. It is not clear if the software programmer who negligently or recklessly coded the AI Robot/Autonomous Vehicle can be found guilty of manslaughter? In the absence of a proper separate legal framework for crimes/offences committed by various actors in an AI operated environment, courts apply legacy rules to affix culpability on a case-by-case basis.

It is quite clear that every AI accident/incident will have multiple actors involved and the responsibility of each one would be different. Detailed examination of these responsibilities would be essential to filter out the act and intention behind the criminal act. It is thus clear that the men who operate these AI machines or are behind them definitely will face an uncertain exposure. Most countries in the world have allowed technology to come up without changing their laws. Time now demands that we have clear cut rules across the world to handle AI machines/vehicles/robots and these rules must definitely lay down the roles and responsibilities of each actor and the consequences if they don't. These changes will have to occur not just in the area where these AI systems operate but also across connected cross functional rules will have to be amended. The day is not far when this will become a reality.

Assessing the Probability of Artificial Intelligence in Criminal Investigation

Faizanur Rahman,[1] Mohd. Amir[2]

Abstract

Advancements in the field of Artificial Intelligence (AI) are conquering unexpected heights. The main idea embodied by AI is to replace humans so as to reduce human effort, and to develop a highly automated society. The benefit is that these automation technologies will take over the tedious, mortifying and dehumanizing jobs, and leave us free to pursue things we like. The scope of AI encompasses various techniques for knowledge transmission, knowledge representation, automated reasoning, and this is used to empower machines to behave intelligently. The purpose of overall data analysis and knowledge augmentation is to make machines learn and solve complex real-life, problems. AI is an ensemble of technologies, interactions and allied platforms which takes part in helping machine to demonstrate intelligence and reasonability.AI has spread its wings in the criminal justice system. AI tools have been launched in order to remove the discrepancies that remain in the criminal justice system. AI has the potential to challenge any number of legal assumptions in the short, medium, and long term. However, the role of AI in criminal justice administration system has remained unaddressed till now despite the increase and development of artificial technologies. The present paper focuses on efficacy of AI to predict crimes and as a criminal intelligence tools that enable the shift from a traditionally reactionary approach to crime-fighting that is more proactive and preventative in character.

1. Introduction

The latest buzzword surrounded by controversies, whether boon or bane for human existence, is Artificial Intelligence (AI). AI has impressively impacted our lives so far, in ways that enhance human health, safety, and productivity. And now, in ways unknown before, AI is also making its presence known in the governance of the administration of criminal justice. There are certain legal repercussions for every technological development that need to be taken into account, and safeguards need to be developed.[3] For instance, in Saudi Arabia, Sophia, an AI robot developed by Hanson robotics, was given citizenship. This has raised many legal issues

[1] Faizanur Rahman, Assistant Professor, Faculty of Law, Jamia Millia Islamia, New Delhi
[2] Mohd. Amir, Research Scholar, Faculty of Law, Jamia Millia Islamia, New Delhi
[3] John McCarthy, 'What Is AI? / Basic Questions' (John McCarthy, 12 November 2017) <http://jmc.stanford.edu/artificial-intelligence/what-is-ai/index.html> accessed 10 January 2021

relating to what can be regarded as a citizen in today's world, and whether it is possible to achieve the concept of technological singularity i.e., humans will no longer remain the smartest beings, without any harm to humans.

It is possible to describe the main issue of AI law using one word i.e., 'Regulation'. Regulation of artificial intelligence is not just complex terrain, it is uncharted territory for an age that transfers the baton from human leadership to the emergence of machine learning, automation, robotic manufacturing and dependence on deep learning. In order to ensure that the functioning of such technology is consistent with policies, existing laws, social norms, ethics and customs, any new development in technology requires certain regulations. Such regulation is also required by AI. Not only is there a need for negative regulation, but there is also a need for such a policy that would help to develop and apply AI technology.[4] AI will be the turning point in humanity's technological evolution, with human reliance on machines and decision-making algorithms never being so profound. Therefore, any document for AI promotion must be aware of the likely AI ecosystem factors that could undermine ethical conduct, affect privacy and undermine the security protocol. The AI promotion strategy is essential. An integral part of any such strategy needs to be appropriate steps to mitigate these risks. As a society, we are now at a critical juncture in determining how AI-based technologies can be deployed in ways that promote democratic values, not hinder them, such as freedom, equality and transparency. And when such a technology is used in the administration of criminal justice, from crime prediction to crime detection; crime investigation to sentencing, then the rights of the parties are significantly affected.[5] The present paper focuses on efficacy of AI to predict crimes and as a criminal intelligence tools that enable the shift from a traditionally reactionary approach to crime-fighting that is more proactive and preventative in character.

2. Understanding Artificial Intelligence

Intelligence is an attribute that allows any object to work in its own mind. A fundamental idea behind AI is that in the near future, the computers can imitate human behaviour. The computer is said to possess AI when computers perform any tasks that would use intelligence if

[4] Nils J Nilsson, *The Quest for Artificial Intelligence: A History of Ideas and Achievements* (Cambridge University Press 2010)

[5] Vick Sahita, '*Future Impact of Artificial Intelligence and Machine Learning (AI/ML) on the Legal Services Industry of India' (Law Lex*, 30 November 2017) <https://lawlex.org/lex-pedia/artificial-intelligence-legal-services/14977> accessed 12 January 2021

performed by humans. The computer scientist, John McCarthy coined the term Artificial Intelligence in the year 1956. According to him, it was the notion of a system that processes and acts on knowledge, so that the outcome is parallel to how a smart person would respond to similar data. It was this reliance and curiosity towards machines that established AI projects in a way that enabled the performance of tasks requiring humanity.[6]

It is a branch of computer science that formulates the ability to automate learning. AI systems are mainly operated by Machine Learning and run by Deep Learning. The reason for its need is the vast data-based services that are prevalent in every industry. It allows computer machines to perform a role solely that would otherwise normally require human intelligence. With AI, the computer is capable of absorbing any change with any independent details. Many industries have already successfully used AI, for example in gaming, speech recognition etc. The significance in the field of law is yet to be established and confirmed because of the complex nature of the legal industry.[7]

AI has already created programs that enhance paranoid schizophrenic scores, or conception, reproduction, and synthetic creature evolution. It has developed programs that can detect fraudulent financial transactions and robots that can clear a laboratory off empty coke tins. There are services that paint pictures, services that do medical diagnosis, training programs, and learning programs. A field where the AI does not have its influence has become really hard to discern. In tournament in 1997, a computer called Deep Blue beat the World Chess Champion, Gray Kasparov. It is almost everywhere, be it an investment, automated weapons and even espionage. By 2020, it is expected to reach the $70 billion. Since the 3rd Revolution is going to be Technological Revolution through AI, and India will lead this revolution, the legal prospect of AI in India is therefore important to understand and discuss.

3. Legal Status of Artificial Intelligence

[6] Stuart Russel and Peter Norvig, *Artificial Intelligence: A Modern Approach* (Prentice Hall Publishers 2009)
[7] Nils J. Nilsson, *Problem-Solving Methods in Artificial Intelligence* (McGraw-Hill 1971)

Assessing the Probability of Artificial Intelligence in Criminal Investigation

The first step towards India's artificial intelligence system was the AI Task Force Report, led by N. Chandrasekaran, Chairman of Tata Sons, to research the use of artificial intelligence.[8] It was set up by the Ministry of Commerce and Industry to make use of AI for financial advantages and to make suggestions on the strategy for sending AI to India. The study of the Task Force, published on 21 March 2018, is a follow-up to the consolidated skills of individuals from different divisions and also analyses how AI can help India.[9]

Following the publication of NITI Aayog's strategy paper on 4 June 2018, known as the "National Strategy for Artificial Intelligence #AIFORALL", India recognized five priority sectors for the use of AI *viz.*, health care, agriculture, education, smart cities and infrastructure, and smart mobility and transport. It also shed some light on topics related to privacy, data protection and ethics and security related to Artificial Intelligence.[10]

Information is one of the main drivers of AI, hence information is to be handled correctly thereby ensuring privacy and security is of primary importance.[11] After the Analytica data controversy, which was a big political scandal, a U.S. political party hired Cambridge Analytica to download information from officials of the opposing party *via* Facebook.[12] Every AI interface is entirely dependent on the data stored within its framework. Unlike other applications where human orders lead to results, AI frameworks construct their decision-making process over time on the basis of mechanical analysis of user data.[13]

---

[8] Pranav Mukul, '*Task force set up to study AI application in military' The Indian Express* (New Delhi, 3 February 2018) <https://indianexpress.com/article/technology/tech-news-technology/task-force-set-up-to-study-ai-application-in-military-5049568/> accessed 11January 2021

[9] Elonnai Hickok, Shweta Mohandas & Swaraj Paul Barooah, '*The AI Task Force Report-The first steps towards India's AI framework*' (*The Centre for Internet Society*, 27 June 2018) <https://cis-india.org/internet-governance/files/ai-task-force-report.pdf> accessed 10 January 2021

[10] Software Freedom Law Center, '*Technology Policy Developments in India: 2018*' (*Software Freedom Law Center India*, 24 December 2018) <https://sflc.in/technology-policy-developments-india-2018> accessed 10 January 2021

[11] Arnab Kumar *et. al*., '*National Strategy for Artificial Intelligence' (Niti Aayog*, June, 2018) <http://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf>> accessed 10 January 2021

[12] Julia Carrie Wong, '*The Cambridge Analytica scandal changed the world – but it didn't change Facebook' (The Guardian*, 18 March 2019) <https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook> accessed 10 January 2021

[13] Yashdeep Chahal, '*India's Unregulated Tryst with Artificial Intelligence: Looking into Future Without A Law?' (Live Law*, 9 June 2018) <https://www.livelaw.in/indias-unregulated-tryst-with-artificial-intelligence-looking-into-future-without-a-law/> accessed 10 January 2021

The right to privacy was held to be a fundamental right enshrined in article 21 of the Constitution of India.[14] The Government of India has set up a Committee to investigate data security problems. The Committee shall draw up an exhaustive system for data security, which is non-partisan innovation and handles conspicuous problems, such as the growth of AI utilization in India.[15]

Given that the development of AI is still at an early stage, it is difficult to differentiate between acceptable legal reactions. There are two schools of thought to create a sensitive regulatory system for AI. It is assumed that static *ex-ante* control does not have the capacity to handle fast-developing technologies such as AI *via* traditional steering instruments. Furthermore, it is hoped that the creation of a framework for a complex administrative system, while innovation is still largely dependent on individuals, would address issues of well-being, morality and transparency and will not pose major challenges to the innovation and expansion of AI.

Artificial intelligence is used without an administrative or legal structure that deals with issues such as risk, information assurance, security and mechanical and security measures. To protect the data of a person, India needs a robust system to govern artificial intelligence.[16]

4. Artificial Intelligence in Criminal Investigation

According to the National Institute of Justice, "any policing strategy or tactic that develops and uses data and advanced analysis to inform forward-thinking crime prevention is part of predictive policing tools." Predictive policing comes in two main forms i.e., location-based and person-based. Both use past policing data as the main driver of these predictions. Location-based predictive policing works by identifying places of repeated property crime and trying to predict where they would occur next. Person-based predictive policing aims to pinpoint who might be committing a crime.[17]

[14] *K S Puttaswamy v Union of India and Ors* (2017) 10 SCC 1

[15] Adithya Anil Variath, '*Changing the Dynamics of Law in India With the Arrival of Artificial Intelligence and Robotics' (T.I. Chronicles*, 5 November 2018) <https://tichronicles.com/2018/11/05/changing-the-dynamics-of-law-in-india-with-the-arrival-of-artificial-intelligence-and-robotics/> accessed 10 January 2021

[16] R. Anand, A. Taneja, and D. Gupta, *Artificial Intelligence* (Bhavya Books 2013).

[17] Hitesh Kumar Reddy, Bhavna Saini, Ginika Mahajan, 'Crime Prediction and Monitoring Framework based on Spatial Analysis' (2018) 132 Procedia Computer Science 696-705

Surveillance tools can be used to watch, track, and store information about a person. This ranges from ring doorbells to facial recognition systems at the border.

Criminalizing algorithms are used in housing, credit determinations, healthcare, hiring, schooling, and more. Many of these have been shown to make recommendations and decisions that negatively affect marginalized communities. The results and data points produced by these criminalizing algorithms affect all of the other tools discussed here.[18]

Risk Assessment Tools are used in almost every state in the U.S. Many use them pre-trial, although they exist at sentencing and in prison management. There are also specific risk assessment tools for different functions in the criminal justice system for instance, risks of domestic violence or juvenile justice, understanding that factors differ as a general criminal risk or a violent criminal risk of rearrest or re-offense in these situations.

Pre-trial risk assessment tools are designed to help defendants and prisoners predict their future behaviour. They use socio-economic conditions, family backgrounds, neighbourhood crime, job status and other factors to predict the criminal risk of an individual. Research has shown that Risk Assessment Tools have disparate effects on results of criminal justice on the basis of the race, race and age of the accused. Often these proprietary techniques are employed in bail, in sentencing and in determining guilt or innocence. Many criminal justice experts have denounced 'risk assessment' tools as opaque and unreliable. Criminal justice algorithms have come under greater scrutiny.[19]

In 2016, the ProPublica investigation tested the COMPAS system adopted by the State of Florida. In particular, the formula was likely to flag black defendants as future criminals. In fact, only 20% of people who were expected to commit violent crimes continued to do so. Whereas 61% of the candidates deemed to have re-offended were arrested for any subsequent crimes

[18] National Institute of Justice, 'Effects of Human Factors on the Accuracy of Fingerprint Analysis' (*National Institute of Justice*, 16 May 2012) <https://nij.ojp.gov/topics/articles/effects-human-factors-accuracy-fingerprint-analysis> accessed 10 January 2021

[19] Odhran James McCarthy, 'AI & Global Governance: Turning the Tide on Crime with Predictive Policing' (*Centre for Policy Research, United Nations University*, 2019) <https://cpr.unu.edu/publications/articles/ai-global-governance-turning-the-tide-on-crime-with-predictive-policing.html> accessed 12 January 2021

within two years. Some risk miscalculations stemmed from incorrect inputs, according to the investigation. The correlation was found to be higher but not too accurate. COMPAS is one of the nation's most widely used algorithms. A validation study of the system was published by Northpointe in 2009 but did not include a predictive accuracy assessment by ethnicity. Without first testing their validity, many jurisdictions have adopted COMPAS and other methods of 'risk assessment' but how their calculations are made has not been shared by Northpointe.[20]

The defense advocates are calling for more transparent sentencing methods. They are unable to challenge the validity of the results at sentencing hearings. Over the last few years, prominent groups such as the Pretrial Justice Institute (PJI) have been strongly advocating the introduction of these instruments and, among many other risk assessments, the Public Safety Assessment has been adopted in almost every state, up from just a handful at the beginning of the decade. In February 2020, however, PJI reversed this position and specifically stated that pretrial risk assessment tools designed to predict an individual's appearance in court without a new arrest, could no longer form part of solution to establish a fair pre-trial system. It is however pertinent to mention here that on March, 2019 Idaho becomes the first state to enact a law specifically promoting transparency in pre-trial risk assessment tools. The law prevents a trade secrecy or IP defense, requires public availability of all documents, data, records, and information used by the builder to build or validate the pretrial risk assessment tool. The law empowers defendants to review all calculations and data that went into their risk score.[21]

5. Status of Artificial Intelligence Technology in India

A working paper called "National Artificial Intelligence Strategy #AIforAll" defines a National AI policy of the Indian government in June 2018. It suggested a two-tiered structure i.e., Centres of Research Excellence in AI and International Centres for Transformational Artificial Intelligence for organizational support to AI science. The Indian Government sees the promise made in AI to greatly improve the provision of public services in the country. India's

[20] Jason Burnett *et. al*., 'Exploring Elder Financial Exploitation Victimization: Identifying Unique Risk Profiles and Factors to Enhance Detection, Prevention and Intervention' (*National Institute of Justice Final Technical Report*, May 2017) <https://www.ncjrs.gov/pdffiles1/nij/grants/250756.pdf> accessed 10 January 2021

[21] Cristiano Rigano, 'Using Artificial Intelligence to address Criminal Justice Needs' (*National Institute of Justice*, 2018) <https://nij.ojp.gov/topics/articles/using-artificial-intelligence-address-criminal-justice-needs> accessed 10 January 2021

healthcare system, while attracting millions of medical tourists a year, is overburdened and under-equipped in rural areas. The Medical Tourism Index 2016 ranks India 5th in the world as a medical tourism destination. India's AI strategy notes that AI can help to create electronic repositories of health data. India is also looking to AI and Big Data to boost financial inclusion and the quality of banking services, and to push a new agricultural revolution.[22]

In November 2019, Gurugram-based start-up Staqu launched the video analytics platform i.e., Joint AI Research for Video Instances and Streams (JARVIS) in Uttar Pradesh to provide a range of services such as violence, intrusion and pick-up detection as well as crowd analysis by tracking CCTV footage. This is a new way to tap AI to generate valuable information from long CCTV footage by fast real-time notifications that would reduce the time required to generate actionable data.[23]

In 2018, the Punjab police started using Staqu's Police Artificial Intelligence System (PAIS) that provides more than a 1 lakh of criminal records in jails across the state, and options such as face scan, text search etc.[24] Similarly, Trinitro is an AI platform that contains a database of approximately five lakh criminals with facial-recognition features has been assisting the police since December 2018 at Uttar Pradesh. Another homegrown artificial intelligence start-up INNEFU, a facial recognition software is assisting the Delhi police since 2017. On similar front, the Odisha police using AI and mobile computing to develop the analysis of crime data. AI tools assisting correctional officers in flagging administrative violations.[25]

6. Conclusion

Progress in technology is taking place at an extremely high pace, and the fact that many wonders about the replacement of human abilities by machines *via* AI is not to be denied. AI is

[22] Vikram Sharma, 'Indian Police to be armed with big data software to predict crime' *The New Indian Express*, (New Delhi, 23 September 2017)

[23] Naveen Joshi, 'The rise of AI in crime prevention and detection' (*Allerin*, 30 November 2019) <https://www.allerin.com/blog/the-rise-of-ai-in-crime-prevention-and-detection> accessed 10 January 2021

[24] Richa Bhatia, '*Top 5 Legal AI Startups That Have Changed the Face of Indian Legal Sector' (Analytics India*, 26 April 2018) <https://www.analyticsindiamag.com/top-5-legal-ai-startups-that-have-changed-the-face-of-indian-legal-sector/> accessed 10 January 2021

[25] Prajakta Hebbar, "Kolkata Police to use AI in Crime detection", *(Analytics India*, 9 December 2019) <https://analyticsindiamag.com/kolkata-police-to-use-ai-in-crime-detection/> accessed 10 January 2021

the need for the hour and the same thing has been embraced by many people in the legal profession. But, like anything else, it also has its advantages and disadvantages, and it is high time that we come up with a proper legal framework that allows us to take full advantage of the legal industry's artificial intelligence and mitigate any risks to which the industry is vulnerable due to the absence of any regulatory legal framework.[26]

AI technology in Indian legal system is at the earliest stage of development. Technological advantages have enormous potential, which will be expedient and economical. It is nonsensical to suppose that this is a threat in the law. AI's ability to substitute manual and clerical work will therefore allow professionals to focus on other significant issues and make optimal use of time. Priority must be given to the personal privacy of individuals, which brings with it the need for censoring machines to monitor and filter such activities and data. For that data protection is needed in such systems with the accountability on the data controllers.

[26] Smriti Srivastava, 'Supreme Court to use Artificial Intelligence for better judicial system' (*Analytics Insights*, 27 November 2019) <https://www.analyticsinsight.net/supreme-court-use-artificial-intelligence-better-judicial-system/> accessed 12 January 2021

HOW AI CAN IMPROVE THE JUSTICE DELIVERY SYSTEM IN INDIA

Sumeysh Srivastava[1]

ABSTRACT:

This paper looks at how technology, and specifically AI can transform the delivery of and access to justice in a positive manner. The theoretical framework briefly looks at the functional approach, as well as a combination of Luhmann's theory of technology and the actor-network framework to understand how the use of technology affects judicial delivery. The paper then groups technologies based on the level of legal sanction required for their implementation and how that affects human agency. The paper does a mapping of the different levels of change that AI can affect in the justice system and looks at practical and implementable examples under each level. The paper also provides a brief analysis of legal reasoning and how it applies to AI systems. Using the grouping of technology explained earlier, the paper looks at whether a similar distinction can be applied to AI as well, while also discussing how AI is different from other technologies used in the justice delivery system. In the section preceding the conclusion, the paper looks at the legal and regulatory framework which needs to be required for AI application in the E-Justice system. In the concluding section, the paper suggests the path forward. In all the sections, specific reference has been made to the consequences of the discussion on the justice delivery system in India, and the conclusion section is limited to suggesting a framework for application in India

Introduction

The Constitution of India, among other things, guarantees certain rights and privileges for its citizens. It guarantees equality before the law,[2] as well as access to free legal aid for everyone.[3] With the aim of establishing a rule of law society in India, the Constitution seeks to ensure that the law applies equally to everyone and no one is denied the opportunity to access the legal system due to lack of means. Access to justice for citizens, and the quality of the same, is now recognized as an indicator of the quality of governance and progress of a society.[4] However, the legal system remains tough to navigate for the lay-person. Laws are written in a language

[1] Senior Resident Fellow at the Vidhi Centre for Legal Policy and Program Manager at Nyaaya.
[2] India Const. art. 14
[3] India Const. art. 39A
[4] 'Goal 16-Sustainable Development Goals' <https://sdgs.un.org/goals/goal16> accessed 14 January 2021.

which is difficult to comprehend,[5] leading to situations where people may be unaware of their rights and remedies available to them in certain situations. Even if people can recognize that they are facing a legal issue, finding quality legal assistance can be prohibitively expensive. At the final step, the gargantuan pendency numbers of India's courts further exacerbate the process of allowing people to access the justice system.[6]

The Government, in the last 10 years has pushed the usage of digitization and technology as a solution to improve different aspects of governance. We can see this happening in the justice system as well. It shows that the state acknowledges the failures and limitations of the existing systems in place, while also recognizing the benefits, in terms of cost, access and efficiency of using technology. While the E-courts projects launched in 2010,[7] looks to integrate ICT in the functioning of Indian courts, two recent projects, namely Pro-Bono legal services and the Tele Law project rely on technology to make the process of interacting with the legal system simpler for litigants.[8] This shows the intention of the state to look at technology based solutions to reduce the justice gap.

Within technologies, we can make two broad distinctive groupings. First, are technologies which mainly deal with the input and output of information, like pens, printers, tablets etc. The second are technologies which support and assist judicial functions, like e-filing. The main difference is that the first group of technologies can be adopted with any explicit legal sanction. A judgement can be written by pen, or on a typewriter. The second group however, does require legal sanction. For example, the e-filing system can only be used after a court accepts and allows it.[9] Similarly, digitally verified documents are valid only because this has been regulated by the law.[10] So, essentially, regulation ensures the usage of technology and also

[5] Sumeysh Srivastava, 'Simplifying the Law for the Citizens of India' *Times of India* (August 2018).
[6] BQ desk, 'India's Pending Court Cases On The Rise: In Charts' (*Bloomberg Quint*, 2020) <https://www.bloombergquint.com/law-and-policy/indias-pending-court-cases-on-the-rise-in-charts#:~:text=India now has almost 4,1%2C 2020.> accessed 14 January 2021.
[7] Shalini Seetharam and Sumathi Chandrashekaran, 'ECOURTS IN INDIA FROM POLICY FORMULATION TO IMPLEMENTATION' (2016).
[8] 'Department of Justice Launches Tele-Law: Mobile Application & Dashboard and Nyaya Bandhu(Pro Bono Legal Services)Mobile Application.' (*Press Information Bureau of India*, 2019) <https://pib.gov.in/PressReleseDetail.aspx?PRID=1565228> accessed 14 January 2021.
[9] Odisha High Court, No.865/2020, (Notified on 11th June 2020)
[10] The Information Technology (Controller of Digital Locker) Rules, 2016

validates that legal command has been integrated within the system being used. Illustratively, the government could decree that only digitally signed documents will be accepted for filing in court. Here, the technology is coded at both ends. The documents will have to be digitally signed and the portal will only accept them if they are. Once their function is defined, the software code of these technologies is designed to remain stable and consistent. The challenge is that this approach may not work for Artificial Intelligence. AI is not one technology. It is a set of different technologies that are a "a growing resource of interactive, autonomous, self-learning agency, which enables computational artefacts to perform tasks that otherwise would require human intelligence to be executed successfully."[11] AI is by its nature always learning and improving and hence not stable.

Application of AI to the justice system.

There are three primary ways in which AI can make have an influence on the justice system.[12]

> First, and at the most basic level, technology is assisting to inform, support and advise people involved in the justice system (supportive technology). Second, technology can replace functions and activities that were previously carried out by humans (replacement technologies). Finally, at a third level, technology can change the way that judges work and provide for very different forms of justice (disruptive technology), particularly where processes change significantly and predictive analytics may reshape the adjudicative role.[13]

In terms of first level change, i.e. supportive technology, AI can automate the process of helping people understand the options available for legal aid and whether they are eligible. An app or programme where a person can enter relevant details, which are then processed in the programme and help in guiding the person if they are eligible for legal aid or not. Further, the user can be guided to the nearest legal aid centre as per their location or given a list of pro-bono lawyers practicing in their area. This kind of entitlement-availability framework has been used

[11] Mariarosaria Taddeo and Luciano Floridi, 'How AI Can Be a Force for Good' (2018) 361 Science 751 <https://www.sciencemag.org/lookup/doi/10.1126/science.aat5991>.
[12] Tania Sourdin, 'Judge v Robot? Artificial Intelligence And Judicial Decision-Making' (2018) 38 University of New South Wales Law Journal.
[13] Id.

by the grassroots organizations for quite some time, and with the addition of AI tech, it can be scaled up, reducing costs and time taken. Of course, such a programme would have utility beyond just legal aid and can also help people understand government schemes and benefits they are eligible for and how to apply for them. This model is already being implemented by Haqdarshak[14] in India and other organizations around the world. Another application that can be imagined here is AI powered translations. When Google switched to neural machine translation,[15] it was supposed to shake up the translation world and make human translations obsolete. Neural machine translation does not translate word for word, and works on predicting the likelihood of a whole sequence of words, creating whole sentences. While translators are still around, anyone who has been using Google Translate for some time will agree that it has really improved to the point where anyone with any decent knowledge of the target language can get by without a translator. This can be challenging for legal documents, because the law often contains terms and phrases in English, for which there is no counterpart in other languages, but the nature of the AI beast functions in a way that the more data it processes and the more it learns, it will improve. Every time you correct a translation in google translate, the AI takes note, and stores the correction in its memory. Legal translations will be tougher and will take time to perfect, it is definitely a possibility for near term application of AI. The Indian Supreme Court has been leading the way with this, with the court starting translation of judicial documents into nine vernacular languages with the help of AI.[16]

In terms of second level change, i.e. replacement technology, there is scope to serve users with first level legal information without sending them to lawyers. If someone has a query and are not sure about which law applies to them or if there is a legal solution to their problem, they should be able to submit the query and get first level information based on AI powered analysis of their data. This will save people a trip to the lawyer and also the cost of the same. More people may be encouraged to enter the justice system if it's easier for them to understand how the law applies to their situation. This will also help people to decide whether they need to go to lawyer

[14] 'Haqdarshak-Every Citizen Matters' <https://haqdarshak.com/home> accessed 14 January 2021.
[15] Shruti Dhapola, 'Google Adds "Neural Machine Translation" for Indian Languages: Here's What It Means' *The Indian Express* (April 2017).
[16] Bhadra Sinha, 'Supreme Court Will Now Translate Daily Orders and Judgments into 9 Languages Using AI Tools' (*The Print,* 2020) <https://theprint.in/judiciary/sc-will-now-translate-daily-orders-and-judgments-into-9-languages-using-ai-tools/429597/#:~:text=New Delhi%3A Daily orders and,intervention in translating judicial documents> accessed 12 December 2020.

at all. Similarly, any interaction with the government, especially in the context of getting entitlements, entails a lot of form filling and submitting certain legal documents. Lawyers often charge a small fee for preparing these documents. This is again something which can be automated based on the information provided by the user, through a software tool which can help people draft legal documents and create pre-filled forms in the proper format.[17] An example of this can be the Civil Resolution Tribunal in Canada[18] which has launched a solutions explorer which gives "free legal information and self-help tools"[19], which includes guided user funnels, an interactive Q and A and information which can help to prepare for proceedings. This can be useful for India where a lack of information of court processes is seen as one of the biggest barriers in approaching the justice process.[20]

Coming to third level change, i.e. disruptive technology, in terms of application to court processes, there are three main functions that AI can perform. The first is in terms of organising information. AI can be used to recognise patterns in documents and files and organize information based on specific parameters. A method of using AI for document investigation is already accepted and in practice in the US[21] and the UK[22]. The second is in terms of advice. AI doesn't just process information, but can also analyse information and provide an answer based on an input query.[23] In Mexico, simpler administrative decision-making is already being supported by AI. For example, the Mexican Expertius system is currently advising judges and clerks "upon the determination of whether the plaintiff is or is not eligible for granting him/her a pension"[24] Similarly, an ongoing study in Netherlands is exploring whether AI can be used to build a tool to support judges in deciding traffic violation cases.[25] The third function is basically

[17] Anna Prist, 'Conversational AI: How Do Chatbots Work?' (*Medium*, 2019) <https://medium.com/voiceui/conversational-ai-how-do-chatbots-work-4f1bfd069013> accessed 14 January 2021.
[18] 'Civil Resolutions Tribunal' <https://civilresolutionbc.ca/> accessed 14 January 2021.
[19] Id.
[20] Aarefa Johari, 'The Indian Justice System Is Too Slow, Too Complex and Too Costly, Says New Study' (*The Scroll*, 2018) <https://scroll.in/article/866158/the-indian-justice-system-is-too-slow-too-complex-and-too-costly-says-new-study> accessed 14 January 2021.
[21] Moore v. Publicis Groupe SA, [2012] 11 Civ. 1279 (ALC) (AJP)
[22] Pyrrho Investments Ltd v. MWB Property Ltd [2016] EWHC 256 (Ch).
[23] Supra 14
[24] Davide Carneiro and others, 'Online Dispute Resolution: An Artificial Intelligence Perspective' (2014) 41 Artificial Intelligence Review 227 <http://link.springer.com/10.1007/s10462-011-9305-z>.
[25] M Van Der Put, 'Kan Artificiële Intelligentie de Rechtspraak Betoveren (Can AI Bewitch the Courts)?', *rechtstreeks 2019 nr 2* (2019).

the one of predicting court decisions, which has been discussed in detail later in this paper- Page 10

Considerations for use of AI in justice delivery systems and related regulation

Irrespective of whether AI automates functions currently performed or delegated by judges, or it assists judges in their work, there are two key questions to consider. First, what should be the role of qualified professionals in the creation of the information provided by AI, and how does one ensure that the information provided by AI is consistent with the text of the law and supervising judgements of the court. This is important, because there have been instances in other jurisdictions of judges rejecting interpretations of the law provided by specific technology systems.[26]

In order to function properly, AI needs Big Data. For instance the digital apple personal assistant, Siri needs to be fed around 100000 pictures of cats before it can recognize an image of a cat with 95% accuracy.[27] A similar number of consistent, clear cases on a specific issue will need to be fed to AI, before it can accurately give a correct decision when it's asked a question on an issue. It is suggested that only a limited number of cases dealt with by the judiciary are circuitous and complicated and the majority are routine. [28]There are many cases which require a first level assessment before being heard, and may even be dismissed before a hearing or decided within one hearing. In these non-complex cases the court decision is straightforward process based on the data supplied and the decision given by the court is mostly a tool for enforcement. Cases where the outcome is predictable and largely certain, can be automated to be handled by AI. However, in cases where the facts are numerous and contradictory, and/or there is a complex question of law to be addressed, the role of AI can be visualized as more of an information management system, where substantial data can be presented to the judge in a convenient format. Most of the conversations around the implementation of a technology like AI also focus on an

[26] Consiglio di Stato. "*Jurisprudence and the challenge of using algorithms in administrative proceedings.*" note to the sentence to the COUNCIL OF STATE - SECTION VI - of 13 December 2019, n. 8472
[27] Luc Julia, *L'intelligence Artificielle n'existe Pas* (FIRST 2019).
[28] AD Reiling, *Technology for Justice: How Information Technology Can Support Judicial Reform* (Leiden University Press 2009).

ethical framework within which AI should operate, irrespective of where it's deployed.[29] If we talk about the use of AI in the administration of justice, then it's suggested that we look at ethical principles for the use of Al in the administration of justice, drafted by the Commission for the Efficiency of Justice (CEPEJ) of the Council of Europe Working Party on Quality (GTQUAL), adopted in 2018.[30] The five principles given are; Respect for fundamental rights, Equal Treatment, Data Security, Transparency and User Control over AI. The last principle becomes particularly important, as the Supreme Court of Wisconsin has recently ruled that judges must explain their logic behind the use of AI tools in making decisions.[31] Another reason for the importance of user control over not just AI, but all technologies is best illustrated by an example from the UK, where an error in a PDF filling form led to the dysfunctioning of technology which measured the economic capacity of parties and went undetected for more than two years and led to incorrect calculations used in multiple cases.[32]

To make AI work in the justice system, other than adherence to ethical principles, there are some other requirements. Clean data sets are needed because the use of incorrect data can affect the efficiency of the working of the AI.[33] The data needs to be machine readable and processable, structured for use in legal proceedings.[34] As discussed earlier, AI needs huge sets of consistent data to be able to start understanding and recognizing the correct information. This type of data sets may not be available in judicial decisions, because even in routine cases, there may be minor variations in the legal and procedural issues and facts. Third, if we want transparency, then we would also want to be able to understand why an AI system gives a specific result. This may not be achieved to a required standard because research shows that AI is still not at the same level as humans when it comes to explaining decisions.[35] This is related to

[29] Vincent C Müller, 'Ethics of Artificial Intelligence and Robotics', *The Stanford Encyclopedia of Philosophy* (2020).
[30] European Commission for the Efficiency of Justice (CEPEJ). *European Ethical Charter on the Use of Artificial Intelligence in judicial systems and their environment*. Strasbourg, Council of Europe 2019
[31] State v. Loomis, 881 N.W.2d 749 (Wis. 2016)
[32] F Contini and GF Lanzara, 'The Elusive Mediation between Law and Technology: Undetectable Errors in ICT-Based Judicial Proceedings' in P Branco and others (eds), *Tools of Meaning: Representation, Objects, and Agency in the Technologies of Law and Religion* (Aracne 2018).
[33] Kristian Lum and William Isaac, 'To Predict and Serve?' (2016) 13 Significance 14 <http://doi.wiley.com/10.1111/j.1740-9713.2016.00960.x>.
[34] Marc Van Opinjen, 'Legislation and Linked Legal Data in the Netherlands' (2017).
[35] Finale Doshi-Velez and others, 'Accountability of AI Under the Law: The Role of Explanation' (2017) <http://arxiv.org/abs/1711.01134>.

the challenge of using AI to replicate the process of legal reasoning. When we talk about legal reasoning, it's important to understand that while the law is not literally a science, in that unlike the subject of physics, which is governed by universal, immutable rules and units, there is still a fundamental logic in how it operates. This has been explained as reasoning by example by Levi.[36] The first step in this process is an original question of law, which when decided becomes the rule of law. The precedent then is applied to the next case which is similar to the original case. The judge's role here is to analyse the similarity in the cases and whether the rule of law decided earlier would apply. This is something which lies within the individual domain of the judge. After this, the judge looks beyond the legal aspect of the case, and analyses the overall context of the case and develops their own interpretation of the case. This is the process that AI seeks to replicate.

In terms of how to regulate integration of AI into justice systems, it is useful to look at the distinctions in technology that has been discussed earlier with examples. First, an illustration can be the use of speech to text technology. This is a widely used application of AI, available in almost all devices.[37] Within the framework of E-justice, speech to text can be used for swift and accurate court hearings and document drafting. Again, the use of speech to text would not require any explicit legal sanction, the text can be verified immediately by the judge as well as the parties and can help to speed up court proceedings. The use of AI is often associated with ethical concerns and a lack of transparency.[38] However, here, as long as the text can be verified and approved, the use of AI can actually help to increase transparency. The agency remains with the person approving the text, like the judge or the clerk, who can be held responsible in case the text has any error.

However, not all potential applications of AI in justice systems are as simple. Let's take a look at predictive justice systems. To be clear, we are not currently at a stage where judicial

[36] Levi, *An Introduction to Legal Reasoning*, 15 U. CHI. L. REv. 501, 501 (1948).
[37] Takialddin Al Smadi and others, 'Artificial Intelligence for Speech Recognition Based on Neural Networks' (2015) 06 Journal of Signal and Information Processing 66 <http://www.scirp.org/journal/doi.aspx?DOI=10.4236/jsip.2015.62006>.
[38] Brent Daniel Mittelstadt and others, 'The Ethics of Algorithms: Mapping the Debate' (2016) 3 Big Data & Society 1 <http://journals.sagepub.com/doi/10.1177/2053951716679679>.

decisions themselves are taken by machines, but the use of AI in predictive analytics has been adopted by certain jurisdictions.

> Just as much legal research makes recommendations (inputs) based on theories about the potential consequences of legal change, the predictions of decisions can be used for downstream analyses of causal evaluation of the effects of decisions. The predictions would not be used to suggest a decision, but used as inputs to increase efficiency and fairness of law[39]

Judicial decisions require judges to make an assessment of relevant facts and regulations before making a decision. The AI system processes data and provides the information to the judge to help them. The final decision would remain with the judge. However, the information provided by the AI may have a suggestive influence on the judge. Another level of this application is to remove the judge from first level decisions, like granting of bail, and hand that over to AI systems.[40] Research shows that current AI systems are not fit to perform this function in an ethical, transparent manner.[41] In the US, the COMPAS system has been adopted different jurisdictions to use predictive analytics to inform judicial functions.[42] Again, research has shown that due to historical data on higher arrests and detentions of the African-American community, the bias is ingrained in the COMPAS system and it's functioning as well.[43] In India, the Crime in India report 2019[44] shows that there is a higher number of people from minority and disadvantaged communities in jail and detention in proportion to their population. So, unless there is a round of data sanitisation done before it's used by AI, we will see the same pattern of algorithmic bias operating in case of use of predictive analytics in judicial functions.

[39] DL Chen, 'Judicial Analytics and the Great Transformation of American Law' (2019) 27 Artificial Intelligence and Law 15.
[40] Shara Tonn, 'Can AI Help Judges Make the Bail System Fairer and Safer?' [2019] *Stanford Engineering Magazine*.
[41] Partnership on AI, 'Report on Algorithmic Risk Assessment Tools in the U.S. Criminal Justice System' (2020).
[42] Equivant, 'Northpointe Specialty Courts' (2017) <http://www.equivant.com/wp-content/uploads/Northpointe_Specialty_Courts.pdf> accessed 15 January 2021.
[43] Julia Angwin and others, 'Machine Bias. There's Software Used across the Country to Predict Future Criminals. And It's Biased against Blacks' (*ProPublica*, 2020) <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> accessed 15 January 2021.
[44] National Crime Records Bureau, 'Crime in India 2019' (2020).

Challenges

There are some basic challenges that need to be understood before any of these suggested applications of AI in justice systems can be implemented. First, for AI to work at scale, legal and civic information needs to be available in machine-readable language. This is not currently the case with legal text in India.[45] However, this is not something which the government needs to be solely responsible for. There are already platforms like Indian Kanoon[46], who have started publishing laws in machine readable format, though at a small scale. The legal position currently is that reproduction and publication of a central legislation along with any commentary or original matter would not be a violation of the government's copyright over the enactment.[47]

Second, is the question of internet access. The latest TRAI data shows broadband level internet is only available to around half of the population.[48] Further, the same data shows that some of the poorest states in India are also worse off in terms of tele density. The India Internet 2019 report[49] shows that rural India has half the internet penetration as urban, and twice as many users who access the internet less than once a week. In this scenario, any legal aid application which seeks to have utility for the actual beneficiaries must have a minimum level of offline functionality. Third, is the questions of digital literacy. The data from the 75th round of the NSSO survey shows that only 20% of the population has the ability to use the internet. The Government's digital literacy schemes are one size fits all and do not track the varying needs and skill levels of different user groups.[50] Any user centric justice delivery application will need to be designed after mapping the skill level and levels of comfort in using technology for users. Serving information in multiple, local languages, as done in the Aarogya Setu App[51] is a good example for this.

[45] Nidhisha Philip, 'Are Indian Laws Really "Open"?' (*Open Knowledge Foundation Blog*, 2017) <https://blog.okfn.org/2017/07/11/are-indian-laws-really-open/#:~:text=The Global Open Data Index,as 45%25 'open'.&text=India has a quasi-federal,government and its various states.> accessed 17 January 2021.
[46] Sushant Sinha, 'Launching Laws of India in the Akoma Ntoso Format' (*Indian Kanoon*, 2019) <https://blog.indiankanoon.org/2019/11/launching-laws-of-india-in-akoma-ntoso.html> accessed 17 January 2021.
[47] Press Trust of India, 'Bare Acts Published by Private Companies Does Not Infringe Govt's Copyright: Centre to Delhi High Court' *The Economic Times* (November 2018).
[48] Telecom Regulatory Authority of India, *Highlights of Telecom Subscription Data as on 31st October 2020*, Press Release no. 101, 2020
[49] 'India Internet' (2020).
[50] 'Key Indicators of Household Social Consumption on Education in India' (2020).
[51] 'Aarogya Setu Mobile App' (*My Gov*) <https://www.mygov.in/aarogya-Setu-app/> accessed 17 January 2021.

These are logistical challenges. There are other issues which are more to do with law and regulation. If AI is to play a role in legal processes, we need to ensure that certain rights which are a part of the legal process are ingrained in the AI system. The Right to fair trial is considered a part of the right to life under Article 21 of the Indian Constitution.[52]How does the system administrator ensure that AI systems follow these rules. For this it's useful to look at how the Council of Europe has developed the Ethics Guidelines' for the use of Al in the administration of justice. These guidelines ensure that different human rights, and specifically Article 6 of the European Convention on Human Rights [53]is inherent in the framework for the deployment of AI in justice systems.

Further, if AI is replacing certain functions performed by qualified legal professionals, how would this fit in with the regulations given in the law?[54] Would the AI need to meet some benchmark 'qualifications' (configuration) to be eligible to give such analysis; and if this is 'replacing' lawyers in some preliminary tasks then would an AI generated document hold the same value as one signed by a registered advocate? Second, there are no exclusive answers in law – lawyers who are more familiar with court craft and other modalities of the law can give better and significantly different legal advice. To what extent is AI desirable at all in this situation considering it can create confusion and conflict from a litigant as well. Thirdly, what institutional and administrative rules need to be complied with/ reimagined/ changed for AI generated documents and drafts to be acceptable? – would an AI stamp hold the same weight as an advocate's assent? Lastly, what is the accountability of the AI in situations where it may malfunction or tender imperfect/incorrect advice causing damage to the litigant?

Conclusion

As we have seen in the preceding sections, the application of AI in justice delivery systems is not a question for consideration in the future, but for the present. In terms of legal regulations, three things need to be clarified by the state. The first is legal authorisation. Specifically, where we have discussed AI functions which can provide legal advice, or generate legal documents, an express authorisation is required for them to be applicable. Secondly, an

[52] Rattiaram v. State of Madhya Pradesh, AIR 2012 SC 1485.
[53] European Convention on Human Rights, art. VI
[54] The Advocates Act 1961

official definition of AI and systems and technologies which can be identified as AI, needs to be adopted for use in the justice system in India, which may need to be updated from time to time. Third, the degree of user control, in the terms of a minimum threshold is defined so that we can always define accountability in terms of functions performed by, and through AI, especially in the case of justice delivery systems which affect the lives of everyone. It is suggested by the author that the best way to clarify and create an enabling regulatory framework for the implementation of AI in the justice system is to create a department, housed within the Ministry of Law and Justice, to work on this. It should have a mixture of researchers, industry representatives, technologists, lawyers and public servants working together. It is also strongly suggested that the department, or authority, as it may be should be created through an enabling legislation. Otherwise, any regulation done purely by an agency, may fall foul of the doctrine of excessive delegation. The Supreme Court of India has opined that the charge of excessive delegation cannot be attracted when it is shown that the legislature has considered a matter, given a definite policy position on it and then leaves it up to an agency to implement that policy,[55] which is the process suggested here.

Using AI to change the justice delivery system in India has benefits for the state, in terms of increasing efficiency of delivery and generating usage data which can be used to improve design and implementation. It has benefits for lawyers in terms of helping people understanding how the law applies to them and legal recourses for their problems. But most, importantly, it has the potential to have a positive effect on how people and communities experience the legal aid system in India.

[55] Mahe Beach Trading Co. & Etc vs Union Territory of Pondicherry, 1996 SCC (3) 741

DELIBERATING THE SCIENCE OF ARTIFICIAL INTELLIGENCE WITH FOCUS ON THE LEGAL ISSUES PERTAINING WITH IT

Anshuman Srivastava[1], Anshuman[2]

ABSTRACT

Artificial Intelligence, as the word suggests is an artificial method of inducting human conscience and intelligence in a machine or a in a certain kind of technology with the help of language coding and various algorithmic deduction. Like any another science, the science of AI has its own pros and cons which in some way or the other affects the human life. But, this unique relationship between humans and machines also give birth to some major legal implications and doubts. This technical relationship has got one major defect that even if it is a machine designed programme, it keeps a human touch within itself i.e. any decision or any agreement made by an AI platform has an human influence in itself and to be precise, it is a human which gets the privilege to decide someone else's modus operandi.

To highlight some of the prominent legal issues, they are – need for algorithmic transparency, problems due to legal personhood, cybercrimes and cyber security concerns, data security and privacy related issues, no accountable authority incase of a breach, deduction of human opportunities from a legal perspective etc. Leaving all these issues apart, there is one issue that raises up several questions which are mostly unanswered; the issue talks about the liability of a certain AI mechanized technology in cases of a crime or tort committed by them. Like, for example according to the US courts any AI mechanized technology or a robot cannot be sued under their law and the same set of practice is followed under the English Law as well. Therefore, this paper reflects those legal issues which needs to be checked upon and to introduce a full-proof AI system in the future.

INTRODUCTION

The most essential characteristic for any field of science in order to gain general acceptance is its quality of uniqueness, i.e. if the output product given by a certain field of science is completely new for the current world, then that specific field has got more chances to prosper in the coming times. Therefore, if we talk about the science of Artificial Intelligence; the

[1] **Faculty of Law, Jamia Mllia Islamia, New Delhi sri.anshuman1505@gmail.com,**
[2] **Anshuman, Campus Law Centre. Faculty of Law, University of Delhi anshul.639.as@gmail.com**

above explained criteria completely harmonize with the science of Artificial Intelligence. Now, if we start from the very basic of how the science of Artificial Intelligence works, we first need to study the meaning of two words i.e. Artificial & Intelligence; so Artificial is something which is a secondary or a duplicate form of the real object and Intelligence is a skill of understanding or a vital sense of acumen. So, now if we combine both these words we will get to understand that AI is a kind of secondary platform through which someone can interpret or solve out any principal problems for which a standard sense of understanding is required in any of the contemporary scenarios possible to happen.[3]

The argument to discuss the credibility of any specific field of science is quite a valid point, as there is always a scope for error which can lead to some unwanted outcomes that can result into some unnecessary disturbances which causes an entire disruption in the ongoing cycle of work or any of the definite activity. In the same way, the science of Artificial Intelligence causes many kind of irregularities in various fields of research, and to be precise the AI interface has got some major legal issues, those if not checked in the coming times can pave the way for some grievous consequences. To describe some of the considerable legal issues related with AI, they are – Cybercrimes and Cyber-threats, Data privacy concerns, lack of proper accountable authority, decrement in the opportunities for persons who are related with the legal field. This modern science brings the human civilization to the verge automation i.e. solving any issue or problem which requires human intelligence, can now be figured out with the help of a machine system that uses algorithmic patterns to solve out any such problems. But, this automation sometimes changes paths by bringing up issues which can cause extensive legal concerns that at-last breaks the properly maintained chain of working discipline. [4]

UNDERSTANDING THE CONCEPT OF ARTIFICIAL INTELLINGENCE

[3] 'What is Artificial Intelligence? How does it work' (Built in) <https://builtin.com/artificial-intelligence> accessed 15 January 2021.

[4] Jake Frankenfield, 'Artificial Intelligence' (Investopedia, 6 January 2021) <https://www.investopedia.com/terms/a/artificial-intelligence-ai.asp#:~:text=Artificial%20intelligence%20(AI)%20refers%20to,as%20learning%20and%20problem%2Dsolving> accessed 16 January 2021.

It all started by a piece of elementary research by **Alan Turing**, a famous mathematician who helped the Allied forces to win the World War 2. His paper titled as, "Computing Machinery and Intelligence" turned out to be the vision light for the modern time AI. Artificial Intelligence expresses the ultimate excellence of human efforts in order to give birth to a completely path breaking invention which can extend the scope of human vision by introducing new dimensions in the field of problem solving and quick responses section. AI tools uses the modern technologies in such a manner, that the out coming results are quite similar to the outcomes given by a human if the same set of problems was presented to him. The machines or the systems that are equipped with these technologies tries to inculcate in itself all the characteristic which a human will show at the time of problem solving or at the time of giving quick solutions to a certain issue at hand. There are distinctions made in the field of AI, so as to help in forming the real perception about what is AI. There are two basic categories, namely; Artificial Biological Intelligence (whose basic work is to amalgamate itself with the particular environment in order to boost the productivity rate) and Artificial General Intelligence (this category can be termed as the classic AI category as its function is to follow the algorithmic pattern to hand out the solution of a given set of problem).[5]

To be clear-cut in our approach towards explaining the in-depth meaning of AI, we can say that when a technically run program adapts the sense of a human or in particular when the program imitates all the functions that are similar to humans, in respect with the actions of the humans that are related with the mind or intelligence aspect; that will be said as the real meaning of the term AI. The main function of AI is to study the given issue at hand in such a manner that the expectancy of a perfect result increases and the expectancy of having getting a wrong solution decreases. The innate science behind the working of AI is 'Machine Learning' which helps the AI programs to learn and get used to, by themselves; for any kind of data set without the help from an outside agent. And, to make this function more accurate the technology of 'Deep Learning' comes into play which helps this function to be done automatically. The science of AI is such an developing piece of excellence that it itself makes a function look extinct, i.e.

[5] Marshal S. Willick, 'Artificial Intelligence: Some Legal Approches and Implications' AI Magzine (Nevada, 1 July 1983) 4.

those functions which were once termed as AI are now accepted as the inherent functions of a particular system, working in any device whether it is Phone, PC, Tab etc.

DISCUSSING THE RELATION BETWEEN HUMANS AND ARTIFICAL INTELLIGENCE

One of the most remarkable inventions that has pushed the limits of human capabilities is of Artificial Intelligence. Humans have always been into producing and creating things that would help them to grow or develop in a very short span of time and by doing this they have reached the limit of helping themselves by the creation of such AI tools which can easily do as much work as they can do and with the same accuracy and productivity as well. These AI systems and tools have helped the humans in every way possible, whether it is economically, politically, scientifically, socially etc. To describe some of the advantages humans have by these AI tools are as follows:--

1. AI systems has acted as a life safer when it comes to healthcare services. The technology has contributed to several apps, websites, chat-bots etc. in order to advice people with the most appropriate health tips and solutions.
2. Making workspace and communication easier by helping translate languages for everyone and helping them to communicate in a much more enhanced and specific manner.
3. Transforming the society into a paper-less society which can help people to reduce red-tapism and taking tough decisions in a much swifter manner.
4. As it is said the introduction of AI tools will result in the reduction of jobs, well one can now say that this not completely true, because it has given to several other vacancies which can help many persons to earn their daily bread.
5. AI has also made a huge impact in the creativity sector (like art and craft, graphic designing, photoshopping, Wallpaper designing etc). These things can now be easily designed due to the inventions of many smart AI tools.

Coverage of Legal and ethical issues with Artificial Intelligence

Deliberating the Science of Artificial intelligence

The advent of Artificial intelligence (AI) has unquestionably raised legal, social and ethical issues for lawmakers, consumers, and businessman who need to be looked upon. Here we will see a few of such issues that are needed to be managed-:

1. **Contract** - There is a drawback in the current legal framework of the contractual liability as machines choose their own counterparts, negotiate contractual terms, conclude, and decide how to implement the contract; traditional rules might become inadequate. Formerly, the software would perform the way it was made to, but when it comes to machines, nothing is stable and keeps evolving. Everything depends on the data they receive; the more they receive, the more they become accurate. Parties to the contract might consider contractual provision which contains agreement like the technology will work as planned and in case of any diversion the contractual remedies will follow.[6]

2. **Privacy** – AI uses a massive amount of data to function, which makes privacy one of the most primary legal issue that users will face while working with it. But the free flow of data is also necessary to utilize the robots to their full potential but it should be in accordance with the Union Legal Framework for data protection. It is completely necessary that robots be developed by giving due care; that they are safe, secure, and follow procedures for data processing, which must be in accordance with the ethics, confidentiality, and existing legislation. Governments in view of the above-mentioned problems are now updating their privacy legislation in order to strengthen privacy concerns and fight against data breaches. Consumers are also now becoming concerned about their mishandling of personal information.[7] In 2015, European Commission conducted a survey which showed 7 out of 10 people had shown concern regarding misuse of their personal data. The European Parliament enacted the General Data Protection Regulation (GDPR), which is a complete set of rules to keep the personal data of all its citizens safe. In GDPR, organizations must

[6] Scarlett trazo, 'Emerging legal issues in an AI-driven world' (LEXLOGY, 17 July, 2019) <https://www.lexology.com/library/detail.aspx?g=4284727f-3bec-43e5-b230-fad2742dd4fb> accessed 15 January 2021.

[7] Mina Krzisnik, 'The Legal Challenges of Artificial Intelligence' (IURICORN, 22 January, 2019) <https://www.iuricorn.com/the-legal-challenges-of-artificial-intelligence/> accessed 16 January 2021.

show transparency while collecting and using the data of the public. Various other countries are yet to enact something like GDPR in order to prevent unauthorized access of data. However, companies like Apple and Accenture in the US have shown interest in making a robust regulatory framework to evaluate and monitor AI systems[8].

3. **Biased and discriminatory effects of AI** – As now many entities have started using AI in their decision-making process, which has sometimes led to some discriminatory and biased results. In 2016, ProPublica, a non-profit newsroom, found out that few US states and cities are using an algorithm for making bail related decision that was totally discriminatory towards black US citizens as it was falsely labeling black prisoners at higher risk of re-offending than white ones. Efforts are made in this area to eliminate discriminatory elements out of the algorithms; for instance, Accenture has made a tool that empowers companies that put an end to racial, ethnic, and gender biasness in their AI software.

4. **Liability** – Currently, we don't have any legal framework that makes robots liable for their conduct like for instance in the case of any damage caused to a third party. But liability depends on the 'Strict Liability' rule of Torts, which says that the test is whether a reasonable person is able to predict the general consequences that would result from his or her conduct, without the benefit of any past knowledge or experience. If the answer is yes, such a person shall be strictly liable for acts or omission of a robot. The Rylands and Fletcher rule, which is also called the 'strict liability' rule, held that the defendant would be liable even if no intention or negligent act has been found out by his side, if it is proven that the defendant's actions resulted in injury to the plaintiff.

   There are also rules for product liability in Tort law, which works only when the AI system in question is a product and not a service. Product liability focuses on

[8] Scarlett trazo, 'Emerging legal issues in an AI-driven world' (LEXLOGY, 17 July, 2019) <https://www.lexology.com/library/detail.aspx?g=4284727f-3bec-43e5-b230-fad2742dd4fb> accessed 15 January 2021.

negligence like negligent manufacturing, negligent design, and violation of the duty to warn. This can make liable one or more parties involved in the manufacturing, sale, and distribution. But these rules of product liability in many cases are proved insufficient as they are unable to figure out the person liable for the robot's act or omission as identifying where the defect occurred in the supply of chain of an AI product is not easy taking into account the evolving nature of the machine learning and algorithm. In order to find a solution, EU Parliament seeks the establishment of a compulsory insurance scheme similar to what already exists for cars and robot owners and producers[9].

5. **Intellectual Property Rights** - According to European Union draft of the European Parliament to the Commission on Civil Law Rules on Robotics "humanity may be at risk of, AI totally superseding human intellectual capacity". To avoid such danger, the report suggested the importance of human maintaining the competency to operate and manage its own control. Various offices granting copyright all over the world has already mentioned that they won't approve work done by machines. This stand became more clear when San Francisco court denying copyright request for a selfie taking macaque monkey. It emphatically held that copyright law only provides protection to the "fruits of intellectual labour" that are "discovered in the creative powers of the mind". Under U.S patent law an 'inventor' is defined as a person or more than one person who discovers the subject matter of the invention which eliminated any hope for patent grant to anyone else than human beings. However EU has inspired nations to take a liberal step by granting copyright to work produced by computer and other devices under the category of own intellectual discovery but nothing has been suggested for parents as such.[10]

European Union recommendations on Artificial Intelligence

[9] Scarlett trazo, 'Emerging legal issues in an AI-driven world' (LEXLOGY, 17 July, 2019) <https://www.lexology.com/library/detail.aspx?g=4284727f-3bec-43e5-b230-fad2742dd4fb> accessed 15 January 2021.

[10] 'Artificial Intelligence: The real legal issues' (Osborne Clarke, 23 October 2017) <https://www.osborneclarke.com/insights/artificial-intelligence-the-real-legal-issues-an-article-by-john-c-buyers-osborne-clarke-llp/> accessed 18 January 2021.

The European Parliament Resolution of 2017 on the Civil Law Rules on Robotics acted as the threshold rules towards the regulation of artificial intelligence. The resolution however, is not binding, but it does offer the European Commission a series of advice that should be taken in the area of artificial intelligence, not only regarding Civil law but also of the ethical aspects of AI. According to the document, a complete union system of registration of advanced robots should be developed, which should be operated and controlled by EU Agency for Robotics and Artificial Intelligence. As for liability, either strict liability, which makes a person liable even if the person is not at fault, or a risk management approach, in which it is ascertained that whether the risk could have been minimized or not. A mandatory insurance scheme for users should be available and a compensation fund to get compensation in case no insurance policy is covering that risk. The resolution proposes code of conduct to deal with ethical issues, and these codes give us four principles: -

- Beneficence – robots should work in the best interests of human beings.
- Non-maleficence – the doctrine of "first, do no harm" in which robots should not harm a human being.
- Autonomy – the ability to make a well informed and un-coerced decision about the terms of interaction with robots.
- Justice – the true and fair distribution of the benefits associated with robotics and affordability of home care and healthcare robots in particular.[11]

CONCLUSION

It will always be challenging to cope up with the evolving pace of the AI system, but as we have seen above that now, various countries are giving due care to the work of AI and trying to keep the human intellectual work priority over the work of AI. AI might prove a detriment in many ways like it can cause a digital divide between and within nations and can also aggravate income inequality. But AI cannot totally be ignored as it is expected that it can do wonders for the economy in the future. As we have already discussed the issues and challenges like (1) Contractual challenges, (2) Privacy, (3) Biased and Discriminatory effects of AI, (4) Liability, (5) Intellectual Property Rights, it has become requisite for the regulatory authorities, AI makers

[11] Maksim Karliuk, 'Ethical and Legal Issues in Artificial Intelligence' (SSRN, 8 October 2019) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3460095> accessed 17 January 2021.

and professionals to come together in order to tackle these challenges so that AI can be successfully implemented in both ethnic and legal way. Authorities need to gain public trust that AI can in no way come in their way and is just developed to reduce their work burden in order to achieve the expected societal goal that AI is beneficial for all. Well informed Consent, high levels of data shielding and privacy, transparency, the fairness of algorithm, cybersecurity, regulatory oversight, and a liability regime for AI are all important factors that need to be addressed in order to successfully create an AI-driven society as nobody has doubts that AI has tremendous potential for improving our societal and orthodox system of living. In March 2018, President of France Emmanuel Macron presented the country's new national artificial intelligence strategy, which includes an investment of 1.5 billion Euros over the next five years to support research and innovation in the field of artificial intelligence. The decision was made, keeping in mind these four specific sectors: the environment and environmental protection; security; transport and healthcare. The reason behind this investment was to check out the potential of artificial intelligence in sectors where companies can play a major role at the global level.

For artificial intelligence, one of the most important issues is the "black-box" challenge in which when the lawyers submit a query to an AI-powered tool, it goes directly into the "black-box," and subsequently AI-based solution provides an answer. Lawyers are no computer scientists or well versed with every technology that is being invented, but they should have at least a basic knowledge of the tool they are using for work so that they can find a discrepancy that the tool might make in relation to the specific case they are working on. Lawyers need to have a little understanding of what's going into the AI tool and what will come out of it and also understand the general operation of the specific AI tool they are working with. This will bring a more harmonious working environment between lawyers and artificial intelligence. When it comes to dealing with the biasness and discriminatory approach of AI, the solution can be, that it should be developed by diverse people and not only by any specific gender like men or any specific community involving only white people. Without diverse people in the team, the makers

might forget to consider opinions or experiences which are apparent to those with different societal experiences.[12]

Artificial intelligence is not perfect – but neither are human beings as they make mistakes too, but AI has the potential to transform the legal profession in so many optimistic ways. If we start delegating tasks that take much of our time to AI tools, then lawyers can free up the time to do the things they do best. It will benefit clients as they will get quick service in a more cost-effective way, and at the same time, it will benefit lawyers who suffer from prolonged hours of work, depression, anxiety, and a high rate of burnout. Lawyers will be able to interact better with their clients and bring out the matter comprehensively, which is reducing day by day.[13] The likely result, at least for now, maybe a legal framework that largely comprises the codes of conduct, voluntary self-regulation, and evolving contractual practices. Giving an electronic personality is suggested by the European Parliament for smart robots, and also, we cannot rebuff this recommendation, as a future regulation, depending on the extent of autonomy conferred on AIs.

[12] DAVID LAT, 'THE ETHICAL IMPLICATIONS OF ARTIFICIAL INTELLIGENCE' (ABOVE THE LAW) <https://abovethelaw.com/law2020/the-ethical-implications-of-artificial-intelligence/?rf=1> accessed 18 January 2021.

[13] Scarlett trazo, 'Emerging legal issues in an AI-driven world' (LEXLOGY, 17 July, 2019) <https://www.lexology.com/library/detail.aspx?g=4284727f-3bec-43e5-b230-fad2742dd4fb> accessed 15 January 2021.

DECIPHERING THE DILEMMA OF OWNERSHIP AND LIABILITY IN THE REALM OF ARTIFICIAL INTELLIGENCE

SARVAGYA CHTRANSHI[1]

Abstract: The advancements in computational creativity with an unprecedented growth of its usage in numerous industries has posed a rather important question for the existing IPR legal framework – who owns the creations of an AI? There have been vague speculations based on the Turing test or awarding the ownership to the creator of the AI itself but this deviates us from the central issue; IPR is a mechanism to promote, facilitate and award 'human' intelligence in the areas of innovation and inventions. The laws have always been structured around humans. The issue arising out of creative machines is that IP institutions like patents and copyrights have not kept up with the creative intellect of the same. The algorithmic approach of computational systems and the sheer complexity and diversity of its process questions the fundamental approach of the Intellectual Property laws. The following research article delves deeper into the questions of ownership, the current scenario of the legal framework and the adequate reforms needed for the successful inclusion of AI creations. The article also brings clarity on a related topic of ascertaining civil or criminal liability to the actions and consequences of an AI's work. This is an instrumental issue in the modern world as the creator cannot simply be held liable in a sense of master-servant relationship for the work of an AI; due to the independence it adopts in collection of data and its subsequent usage. This would further translate into necessary changes being introduced in the supporting legal framework. Hence, the following article offers an imperative and substantive analysis of the stated issues.

INTRODUCTION

The idea of intelligent machines with humanlike characteristics and abilities has, for a long time, fascinated both the general populace and technological experts alike. Homer had described self-assembling tripods created by the Greek god Hephaestus around three thousand years back. Science-fiction has extensively explored this idea, right from the movie 'Metropolis' in 1927 to Isaac Asimov's book 'I, Robot' in the year 1950. The term 'Artificial Intelligence' (hereafter referred to as 'AI'), however, was first used by John McCarthy while

[1] STUDENT, GUJARAT NATIONAL LAW UNIVERSITY

addressing the Dartmouth Conference in the year 1956.[2] The concept has come a long way since then and is currently in flourishing existence.

Geoffrey Jefferson, a neurosurgeon, had stated in 1949 that,

"Not until a machine can write a sonnet or compose a concerto because of thoughts and emotions felt, and no: by the chance fall of symbols, could we agree that machine equals brain-that is, not only write it but know that it had written it."[3]

Reality is not far from such considerations. Programmes and inventions like Google's AI Eye Doctor, capable of identifying diabetic retinopathy and J.P. Morgan Chase's Contract Intelligence (COiN) Platform using AI to analyse legal documents to the humanoid – Sophia and self-learning machines beating world grandmasters at their games are just few of the many examples. Inventive AI has been able to compose sonnets[4], create paintings and even perform remote surgeries.[5] To produce innovative creations that have a certain standard of exclusivity and originality, computational creativity systems in AI use a variety of algorithmic techniques, including genetic algorithms, simulated annealing, stochastic sampling and filtering, and deep neural networks. The details of the working of these techniques are not as important as the fact that they are capable of inventing. It is in such a scenario, when AI is getting involved extensively in our day-to-day lives, that a legal framework regulating these creations is absolutely necessary.

The World Intellectual Property Organization (WIPO) explains Intellectual Property (hereafter referred to as IP) as –

"Intellectual property (IP) refers to creations of ***the mind****, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce."*[6]

---

[2] John McCarthy, 'What is artificial intelligence?' (*Stanford University*, 12 November 2007) <http://jmc.stanford.edu/articles/whatisai/whatisai.pdf> accessed 25 January 2021

[3] Geoffrey Jefferson, 'The Mind Of A Mechanical Man' (1949) 1105 Br Med J. 1105, 1110

[4] Dom Galeon, 'The World's First Album Composed and Produced by an AI Has Been Unveiled' (*FUTURISM* 21 August 2017) <https://futurism.com/the-worlds-first-albumcomposed-and-produced-by-an-ai-has-been-unveiled> accessed 25 January 2021

[5] Meghdoot Sharon, 'Gujarat Doctor Makes History, Performs World's 1st Robotic Heart Surgery 30 km Away from Patient' (*News18*, 05 December 2018) <https://www.news18.com/news/india/gujarat-doctor-makes-history-performs-worlds-1st-robotic-heart-surgery-30-km-away-from-patient-1961729.html> accessed 25 January 2021.

[6] 'What is Intellectual Property' (*World Intellectual Property Organization* 2020) <https://www.wipo.int/publications/en/details.jsp?id=4528> accessed on 25 January 2021

The expression of 'the mind' speaks of the fundamental issue here – it refers to the human mind as in creations born from the human intellect; the whole idea of IP was to reward the human creator and the 'human' part is what has to be done away with while designing a framework that deals with AI. The following article shall analyse the existing system of Intellectual Property rights and reasonably establish why it will not be suitable for the works of an AI in word or spirit. While evaluating the existing position, it is essential to note that ownership is not just a provision to determine monetary compensation. Its application extends to legal rights, resolution of disputes and very importantly, in ascertaining liability. The current position of the law pertaining to this subject, awards the ownership of the creation to the creator of that AI software. But AI is not a conventional tool built to aid an individual; it can be sufficiently autonomous in its functioning. Thus, it is unreasonable to ascertain the liability of its act to its creator. Conclusively, it would be an exceedingly convenient position to adopt if the status of ownership changes with the purpose, therefore, it is imperative to discuss it in accordance with the issue of determining liability. The following article further attempts to suggest a plausible course of action.

CURRENT LEGAL FRAMEWORK AND RELATED FLAWS

COPYRIGHTS AND PATENTS:

A copyright is a legal right that basically awards ownership and protects the ingenuity of creations born from the human intellect. The WIPO says that –

> *"Copyright (or author's right) is a legal term used to describe the rights that creators have over their literary and artistic works. Works covered by copyright range from books, music, paintings, sculpture, and films, to computer programs, databases, advertisements, maps, and technical drawings."*[7]

Section 14 of the Indian Copyright Act 1957[8], defines 'copyright' as the exclusive rights of owner to do or authorise the doing of any acts (such as reproduce work, publication of work, adaptation and translation etc.) in respect of a work.

A patent is however, an exclusive right granted for an invention, which is a product or a process that provides, in general, a new way of doing something, or offers a new technical

[7] 'What is Copyright' (*World Intellectual Property Organization)* <https://www.wipo.int/copyright/en/faq_copyright.html> accessed on 25 January 2021
[8] Indian Copyright Act 1957 (India)

solution to a problem.[9] It is essential here, to disclose the technical information about the invention in public domain for a patent claim. Patents are exclusive to inventions and therefore, govern a niche area compared to copyrights.

The purpose of these instruments is what the entire system of Intellectual Property Rights (hereafter referred to as IPR) is based on – to incentivise creators to develop products that benefit the society and ensure in the process that there is no infringement or misappropriation of the same by anyone else. It is important to note here that copyrights can be obtained for the expression of ideas and not the idea itself. This means that there should be a tangible creation arising out of an original idea that can be owned under this instrument. Since the applicability of copyrights is generally wider in the current AI scenario, our discussion will be focused on the same.

EXISTING JURIDICAL POSITION:

There are certain requisites to obtain a copyright, most important of them being the concept of 'authorship'. This means that the person claiming the copyright must be the author himself i.e., the original creator or must have succeeded to the rights of the author. In the case of patents, section 6(a)[10] of the Indian Patent Act allows patent application by any person claiming to be the true and first inventor of the invention. These definitions make it seem plausible for an AI to be awarded the 'ownership' of its creations. However, there are major issues in this consideration; the first being that these laws are meant for human beings. The provisions in the Copyright Act speak of the human element. In the case of Diamond v. Chakrabarty, the US Supreme Court had observed that *"anything under the sun that is made by **man** is patentable".*[11]

Various jurisdictions in the world have made it clear, as of now, that they are not willing to grant ownership to anyone or anything other than humans. The Court of Justice of the European Union in its decision of Infopaq International A/S v. Danske Dagbaldes Forening[12] stated that copyright only applies to original works, and that originality must

[9] 'What is a Patent', (*World Intellectual Property Organization*) <https://www.wipo.int/patents/en/#:~:text=What%20is%20a%20patent%3F,technical%20solution%20to%20a%20problem.> accessed on 25 January 2021

[10] Indian Patent Act 1970 (India)
[11] Diamond v. Chakrabarty, 447 U.S. 303 (1980)
[12] Infopaq International A/S v. Danske Dagbaldes Forening, ECR I-6569 (2009)

reflect the *"author's own intellectual creation."* This emphasizes the role of the author's personality which cannot be attributed to an AI software. Similar is the case with patents awarded for an invention where the 'conception of an idea' is an important factor in deciding the award. The US Copyright Office has also held the position of not awarding ownership to exclusive AI creations unless they can be attributed to a human author; autonomous creations just fall into the public domain. American law has a history of not being willing to attribute ownership to anyone other than human, not even animals, as in the case of Naruto v. Slater[13]. The Australian case of Acohs Pty Ltd v Ucorp Pty Ltd[14] had also iterated that a work produced by computer intervention cannot be protected by copyright since it is not produced by a human being. Few other jurisdictions like that of UK, India, Ireland and New Zealand award the ownership to the programmer himself. Section 9(3) of the Copyright, Designs and Patents Act (CDPA)[15] in the UK states –

> "*"In the case of a literary, dramatic, musical or artistic work which is computer-generated, the author shall be taken to be the person by whom the arrangements necessary for the creation of the work are undertaken."*[16]

Although the Indian stance is ambiguous, it is similar to the English law; as reflected in the decision of the Hon'ble Supreme Court in Rupendra Kashyap v. Jiwan Publishing House Pvt. Ltd[17] –

> "*in the context of question papers for an examination, that the author of the examination paper is a person who has compiled the questions; the person who does this compiling,* ***is a natural person, a human being, and not an artificial person****; Central Board of Secondary Education is not a natural person and it would be entitled to claim copyright in the examination papers only if it establishes and proves that it has engaged persons specifically for purposes of preparation of compilation, known as question papers, with a contract that copyright therein will vest in Central Board of Secondary Education."*

There is also the essential feature of originality in the Indian law. It is judged on a set of doctrines that were laid down by the Hon'ble Court as the word 'original' is not explicitly

[13] Naruto et al v. David Slater, No. 16-15469, 2018 WL 1902414 (9th Cir. Apr. 23, 2018)
[14] Acohs Pty Ltd v Ucorp Pty Ltd, FCA 577 (2010)
[15] Copyright, Designs and Patents Act 1988
[16] Andres Guadamuz, 'Artificial Intelligence and Copyright', (*WIPO Magazine*, October 2017), <https://www.wipo.int/wipo_magazine/en/2017/05/article_0003.html.> accessed on 26 January, 2021
[17] Rupendra Kashyap v. Jiwan Publishing House Pvt. Ltd, [1996] (38) DRJ 81

defined in the Copyright Act. The position held by various jurisdictions restrict the discussion on the ownership of an AI, even a partial one. Apart from the fact that they are unwilling to go beyond humans as owners, other provisions and definitions should be judged in the context of AI creations.

AI AND THE CRITERIA OF OWNERSHIP:

Although, the Turing Test is the bellwether in determining the autonomous nature of intelligent machines (it is more relevant from a technological viewpoint rather than a legislative one)[18], here we analyse the specific requirements that an AI would have to fulfil from a viewpoint of gaining ownership of its work. The present examples are capable of it, at least to some extent and refraining from acknowledging that puts us at a disadvantage of furthering the purpose of IPR i.e., to facilitate creation.[19] The moral question of complete ownership in cases of a substantive computer intervention must also be put up; complete liability for the acts of an AI would not be entertained and thus, legally acknowledging its role is important. Also,the extent to which the AI has been successful in fulfilling the criteria of originality should be assessed in the existing legislative terms.

Doctrine of Merger

This doctrine questions whether the idea and expression are intrinsically connected. This is one area where AI might not be fulfilling the requirements as the idea for the outcome will most probably be fed into the system by an external source, herein a human. However, the connection of the individual to the final result is also an issue of contention. Experts have said that developers using AI might not be certain about the result, even in the closest of proximity. For example, a computer programmer could develop an AI software that produces music on its own accord but would not have any idea about music or its production himself. It is in such a case that the result would not be definitively related to the idea coming from the 'source'.

Sweat of the Brow Doctrine

To determine whether the work was created with skill and labour by the author, the 'sweat brow' doctrine is used. Machines certainly do have the required skills and put in

[18] Lance Eliot, 'Turing Test and the Practice of Law: The Role of Autonomous Levels of AI Legal Reasoning', (*Research Gate*, August 2020) <https://www.researchgate.net/publication/343735379_Turing_Test_and_the_Practice_of_Law_The_Role_of_Autonomous_Levels_of_AI_Legal_Reasoning> accessed on 27 January, 2021

[19] Somaya, Deepak, and Lav R. Varshney. 'Ownership Dilemmas in an Age of Creative Machines' (2020) 36 Issues Sci Technol, 79-85

effort to accomplish a goal, maybe not just in the sense that humans understand it to be. Especially, AI machines are specifically more advantageous because of their expertise in specific fields that far exceed human capability. If we are willing to consider this, there is certainly a substantive amount of both skill and labour involved on the part of intelligent machines in any of their creations.

Modicum of Creativity Doctrine

Indian law stresses on a minimum degree of creativity that should be involved with a piece of work to grant ownership rights for it. Several works of different AI software and machines have successfully produced work that did not exist previously[20]. The algorithmic approach that they adopt mimics human creativity to a seemingly indistinguishable extent.[21]

Skill and Judgment Test

Another aspect where there would be a grey area regarding AI would be in determining whether the work is created with mere skill and labour or whether the work possess skill and judgment. Although inventive AI does substantively use its decision-making skills in the production of its wok, it might not be the case at the inception of the act. However, if we keep that discussion reserved for the Doctrine of Merger, inventive AI would not have a problem in satisfying the requirements of this doctrine.

The tangibility of a work is another important aspect covered under the American Copyright Law and the last one in determining ownership rights for a work. The American Copyright Act says that a work is in a tangible medium[22] of expression –

"when its embodiment in a copy or phono record, by or under the authority of the author, is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration."

The tangibility of a work is a loosely based consideration since it is only based on the permanence of expression. Tangible form is not even limited to actual physical form but a

[20] Rebeca Sarai G.G., 'This is an AI-generated artwork of a person who doesn't exist.' (*Medium*, 24 September 2020) <https://medium.com/datadriveninvestor/this-is-an-ai-generated-artwork-from-a-person-who-doesnt-exist-f81b224984f0> accessed 27 January 2021

[21] Sam Daley, '19 EXAMPLES OF ARTIFICIAL INTELLIGENCE SHAKING UP BUSINESS AS USUAL' (*Built In*, 19 December 2018) <https://builtin.com/artificial-intelligence/examples-ai-in-industry> accessed 27 January 2021

[22] Bleinstein v. Donaldson Lithographing Co., 188 U.S. 239 (1903)

way to establish the stability of the work. It implies that to qualify as a tangible form of work, an AI can produce it, even in a soft copy but in a manner that it stays stable for a possibly long period of time. In Tata Consultancy Services v. State of Andhra Pradesh[23], computer programs were held to be tangible. It was held in MA1 Systems Corp. v. Peak Computer, Inc.[24], that the loading of software into a computer's random-access memory was sufficiently permanent for it to be deemed fixed. Such functions are what an AI is sufficiently capable of and are thus, capable of producing tangible work.

ASCERTAINING LIABILITY:

Legal liability is basically the responsibility of an injury that arises out of a committed action or the omission of performance of a duty. It arises primarily in three general classes of wrongs i.e., crime, tort and breach of contract. The discussion on this subject can stretch out for pages but we limit ourselves to the tort of negligence[25] as an essential example that shall lead us to the issues that shall crop up while including AI in its domain. The tort of negligence can be committed on an individual's own accord but another factor that should be considered here is that of a master-servant or employer-employee relationship. AI being used as an aid to an individual which agreeably surpasses the domain of a tool can be treated as an employee or a servant that serves its owner and acts on his command. Although the goal may be pre-registered but the manner of achieving it, would be an original 'thought' of an AI machine and thus, different from a mere tool.

The concept of strict and vicarious liability become very relevant here. Both of these are forms of liabilities that arise without a necessary intent to harm or *mens rea*. The former is applied in cases where there is a 'reasonable foreseeability' for the danger that an object or activity poses. As specific corporate companies are primarily involved in the development of an AI, a sub-category of strict liability which is the strict product liability – arising in cases of a defective product must be stressed upon. The latter arises in cases of an act of a third party, for which the principal party is held responsible. The third party can be an employee or a servant that acts in 'the scope of his employment'. In spite of these instruments being developed for human interactions, some of them can be currently applied to human-AI

[23] Tata Consultancy Services v. State of Andhra Pradesh, [1997] 105 STC 421 AP
[24] MA1 Systems Corp. v. Peak Computer, Inc., 991 F.2d 511 (9th Cir. 1993)
[25] G. Steven Tuthill, 'Legal Liabilities and Expert Systems' (1991) Vol 6 Issue 3 AI Expert 45, 51

interactions. This is essential considering the independent nature of an AI, which makes it unreasonable to treat it as a tool which is in complete control of a human being.

ISSUES WITH THE INVOLVEMENT OF AI:

The primary issue arising with the work of an AI is patent infringement. Inventive AIs need minimum assistance and human intervention in their work to produce unique products (which are not prior art). AI works on collecting data, reorganising and 'understanding' it through algorithmic means and neural networks to produce results. It is highly likely that it can result in a machine infringing an independent patent. One such example is that of the 'Inventive Machine' built by Dr. John Koza.[26] The results that the machine had produced did have instances of patent infringement. The current legal framework does not however, recognise non-human entities for infringement but in the case of AI, working autonomously, it would be very difficult to trace the liability back to its owner because of his limited or no involvement in the process and definitely not in the result.

Another possibility is in the case of criminal liability. The current system basically depends on two elements to validate a crime i.e., *mens rea* (criminal intent of the mind) and *actus rea* (the act of the offence itself). It would not be difficult to associate the latter with an AI but it is considerably difficult, at least in the current system, to prove a criminal intent of the mind on the behalf of an AI. Now this can be viewed in the following circumstances. First, is the AI working on an explicit order given by its owner where the aim to be achieved is wrong in itself. The owner can be simply held liable for the cause. Second, is the case of an innocent motive characterised by a crime committed in the process of achieving it.[27] This is the most probable case in the context of an AI; like the death of the Japanese factory worker who was killed by an AI robot seeing him as an impediment in the realisation of its ultimate goal.[28] The third case is of ascertaining complete liability to an AI driven machine. Self-driven taxies my well be an example of completely autonomous machines that literally work

[26] Jonathon Keats, 'John Koza Has Built an Invention Machine' (*Popular Science*, 19 April 2006) <https://www.popsci.com/scitech/article/2006-04/john-koza-has-built-invention-machine/> accessed 27 January 2021

[27] Weng Y-H, Chen C-H and Sun C-T, 'Towards the Human-Robot Co-Existence Society: On Safety Intelligence for Next Generation Robots' (2009) 1 Int J Soc Robot 267, 273

[28] Robert Whymant, 'From the archive, 9 December 1981: Robot kills factory worker' (*The Guardian*, 9 December 2014) <https://www.theguardian.com/theguardian/2014/dec/09/robot-kills-factory-worker> accessed 27 January 2021

without any human intervention.[29] They can be held completely liable for their acts but then the question of tracing this back to its manufacture arises. If this approach is adopted, it may well discourage the development in this field as a complete and definite prediction for an intelligent machine cannot be made. This final case also raises numerous issues in terms of defences. Could a malfunctioning program claim a defence of insanity? Or the one effected by a virus, that of intoxication (the Trojan Defence)?[30]

In the light of AI production being mostly monitored by big corporates as of now, can the liability be traced back to them? Two concepts of negligence and breach of warranty must be invoked here. The tort of negligence has three criteria to be fulfilled for a successful claim –

1. The defendant had a duty of care.
2. The defendant breached that duty.
3. That breach caused an injury to the plaintiff

.

The first aspect being easier to prove as a software vendor, a corporate in this case must have some standard of responsibility when an AI system is being sold by them. A breach of duty can occur in various ways giving rise to product liability in itself (in cases of erroneous programs) or the inability to gather and process the correct data, in the correct time. An injury can be claimed in the case of the user being charged with any liability on behalf of the program or its act/work per se.[31] Another concept to be applied here is the breach of warranty. If an AI machine is being sold as a product or as an integrated part of the product (in self-driven cars or software applications) then it must be done with a warranty. It shall arise due to an implied contract between the supplier of the product and the end user.

However, ascertaining complete liability to the producer might necessarily not be a reasonable approach as an AI machine serves numerous clients at a time and the user must also be responsible for the work, if not as an owner, then as an employer.

[29] James Jin Kang, Mohiuddin Ahmad, 'Robot take the wheel: Waymo has launched a self-driving taxi service' (*The Conversation*, 15 October 2020) <https://theconversation.com/robot-take-the-wheel-waymo-has-launched-a-self-driving-taxi-service-147908> accessed 26 January 2021

[30] John Kingston, 'Artificial Intelligence and Legal Liability' (*Research Gate*, November 2016) <https://www.researchgate.net/publication/309695295_Artificial_Intelligence_and_Legal_Liability> accessed 27 January 2021

[31] Gerstner M.E., 'Comment, Liability Issues with Artificial Intelligence Software' (1993) 33 Santa Clara L Rev 239 <http://digitalcommons.law.scu.edu/lawreview/vol33/iss1/7> accessed 27 January 2021

This brings us to a viable solution that can be adopted to tackle this problem. The concept of strict liability in cases of a user being adjudged as an employer and the machine as an employee. A 'scope of employment' doctrine must be adopted in case of a machine working for the purpose that it should and without a specific error that can be traced back to the supplier/producer. Any other offences committed by the machine that fall outside the ambit of 'scope of employment' can therefore be ascertained to the original owner. The European Parliament Resolution on Robotics had taken a stance on the matter by stating that an AI cannot be held liable and liability has to be traced back to a human agent which could be the owner, user or the developer if they could have foreseen and avoided the infringement. Their liability should be proportional to the actual level of instructions and training given by them to the AI machine. [32] This is for the time being, as AIs cannot independently compensate or act as a necessarily complete autonomous entity. However, it is not a possibility that is very distant into the future. A framework where the concept of an AI being a legal entity with laws governing its conduct must be given careful thought.

LEGAL PERSONHOOD

CAN AI BE A LEGAL ENTITY?

The current legal framework does not allow for AI to be considered as an independent legal entity. The arguments are many but they necessarily revolve around the fact that AI as a whole is not close to emulating a real person. It might be autonomous in its intellect or display expert niche knowledge but those are not the requisites to adjudge it as a legal person. An AI machine lacks critical human qualities including but not limited to consciousness, feelings, intentionality, desires and the basic sense of awareness of itself.

The expression that robotic weapons (example of AI machines) are not responsible agents is reflected in an act – the Law of War Manual of the United States Department of Defence in its provision 6.9.5.3 states that –

"Law of War Obligations of Distinction and Proportionality Apply to Persons rather than the Weapons Themselves"

The article of the manual proclaims that –

[32] European Parliament, 'European parliament resolution on civil law rules on robotics adopted on 16 Feb 2017' (*European Parliament*, 16 February 2017) <https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html?redirect> accessed 26 January 2021

"the law of war does not require weapons to make legal determinations, even if the weapon (e.g., through computers, software, and sensors) may be characterized as capable of making factual determinations, such as whether to fire the weapon or to select and engage a target."[33]

However, the manual is also a recommendation on International Humanitarian Law and its interpretation. The interpretation can evolve over time and the expression 'does not require' should not mean a complete ban (must not be interpreted as 'it cannot'). The counter arguments also include fact that several other objects or conglomerations have been bestowed with legal personhood under the legal system. Corporations, environmental features and even idols are conferred with the status to include them in the system of rights and obligations. The concept of treating deities, with their own rules, legal obligations and most importantly, rights is adopted numerous times in India. A legal entity might necessarily not be exactly like a human being but the status gives it the basic characteristic to sue and be sued. Thus, on a theoretical and formal level, there are no real barriers to confer AI with legal personhood.

The European Parliament adopted a draft resolution on the matter which would be helpful in determining the future course of action. The draft resolution envisages giving robots the status of an "electronic identity", which has specific rights and obligations. It noted that robots cannot be considered as a mere tool in the hands of humans and complete autonomy over them should not be provided. A similar example to this proposition is that of a foetus' relationship with its mother. The Session of the Council of Europe on Bioethics (December 1996) stipulates that during the entire intrauterine development, the foetus cannot be considered either a part of the body of the pregnant woman, or be regarded as an organ of the future mother. [34] This raises an essential question on whether AI robots be considered as attributed to human beings. The resolution however iterated few guidelines that shall take care of the environmental, social and moral impacts of the AI technology. Development of the technology under these guidelines would be a supportive measure along with the developing legal framework.

[33] U.S. Department of Defense, 'Department of Defense Law of War Manual, 6.5.9.3' (*U.S. Department of Defense*, June 2015), <https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190> accessed 27 January 2021

[34] Council of Europe on Bioethical Matters, 'Texts of the Council of Europe on bioethical matters Volume II' (*Council of Europe*, April 2014) <https://www.coe.int/t/dg3/healthbioethic/Texts_and_documents/INF_2014_5_vol_II_textes_%20CoE_%20bio%C3%A9thique_E%20(2).pdf> accessed 28 January 2021

ISSUES IN AWARDING OWNERSHIP TO AI:

Even if we consider the possibility of ownership being awarded to AI, it would not be practically feasible. The fundamental basis of legally recognised ownership is the incentive that it provides the creator to further invent. An AI is not capable of recognising the incentive and therefore, would not be able to exercise any of its rights. Even legally, the current system does not recognise AI as legal entities and therefore they do not have the standing to own their work.

An alternative to this system is to associate a human owner or moreover, a 'caretaker' that perhaps does not expressly own but takes responsibility for the work of an AI. The concept is already implemented in that of a *Shebait* for a deity in Indian law. As the Hindu Succession Act says, the person or *Shebait* shall represent the maintenance of the work and its management thereof. Any legal proceedings could then be initiated in the name of an AI machine and its work.[35] As the Hon'ble Supreme Court has held in Prafulla Charan v. Satya Charan[36], that the property dedicated to an idol vest in it, is an ideal sense only; ex-necessities, the possession and management has to be entrusted to some human agent, called Shebait. Such a mechanism could work for an intelligent machine too and it deserves legislative thought. An AI can also be a joint inventor vesting the rights accredited to it in the person that is currently associated with it. Complete ownership of an AI seems to be a distant thought for now and future circumstances shall guide legislative work in this direction. Currently, the issue arising out of the human ownership is the determination of the correct person that should be endowed with these rights.

SUBSEQUENT ISSUES WITH HUMAN CONTROL AND CORPORATE MONOPOLY:

The two prime contenders for the ownership rights are the developer that in a sense, owns the machine or the user that is concerned with the specific result produced by the machine. For instance, IBM's Watson is capable of interacting with many users at the same time and IBM has made it available to medical sectors also. The scenario in assigning the ownership rights to the user shall provoke IBM to restrict user-access and decrease the 'creative' possibility of the Watson. On the other hand, ownership can be entrusted with the parent company itself i.e., IBM. The AI, in this case, the Watson shall invent or create under

[35] Hindu Succession Act 1956 (India)
[36] Profulla Chorone Requitte & Ors. v. Satya Chorone Requitte, [1979] SCC (3) 409

its command and the ownership of the work shall stay with the company. This shall expedite progress but it places too much power in the hands of the corporate and induces a sense of monopoly over the technology.[37] If unfettered development in the field of AI is the demand of the time, then in spite of its drawbacks, the latter proposition of vesting patent rights in the owner of the AI machine seems preferable.

This proposition also seems plausible and advantageous to developers and programmers.[38] Now, AI is certainly capable of giving results that exceed the capability of the creator, so much so, that the idea of the final result would also not belong to the developer. But it cannot be said that there is no input from the 'author', in this case, the programmer or the developer in the generation of that 'specific output'. There is the job of determining the appropriate model that shall work with the framework to create the necessary algorithm. Data analysis and programming are two key components of an algorithm (speed and accuracy depends on the bias and variance, respectively)[39] of an AI and a developer spends considerable time to produce it. Conclusively, a lot of time and effort is required to make an AI capable of working like it does. The fruits of this labour can be reaped by the developer in the sense of an employer-employee relationship as stated before.

There's an approach to place the work of an inventive AI in the public domain. This is the approach that is taken by the United States of America currently and there is not much support for it. However, it is an idea that should be further thought upon. The primary reason why it does not actually suit the requirement of the time is because it would restrict the incentivisation for developers. Further, it would be hard to locate the creator of some work and differentiate between that of an AI and that of a human being. The idea works well for the purpose of research and resolving conflicts (governmental control over the creations is a minor addition that could be made to this idea) but shows no scope for the future.

[37] Ryan Abbott, 'I Think Therefore I Invent: Creative Computers and the Future of Patent Law' (2016) 57 B C L Rev 1079, 1115
[38] Samantha Fink Hedrick, 'I "Think" Therefore I Create: Claiming Copyright in the Outputs of Algorithms' (2019) 8(2) JIPEL 324
[39] David Lehr & Paul Ohm, 'Playing with the Data: What Legal Scholars Should Learn About Machine Learning' (2017) 51 U C Davis L Rev 653, 683-84

CONCLUSION

There is a definite need to develop an extensive legal framework for Artificial Intelligence and its interaction with human beings. The uniqueness of this technology and its operations pose unprecedented complications for the regulators; AI could well be the next most intelligent species on the planet and could surpass humans as well. We need to realise that intelligent machines are not an idea for the future, all of us are well surrounded by them. The aspect of ownership and liability have been the two of the most important and fundamental issues in the conduct and creative independence of human beings. In the context of human relationship with the work of an AI, the two are integrated in terms of the questions they pose for the policy-makers.

The concept of IPR was developed to foster the growth and development of our race. When we as a community have set out to create something that must mimic our own intelligence, these issues become equally important in its context too, especially, when AI is intricately involved with our day to day lives. Institutional thought has been given into this, whether it is the report of the NSTC Committee on Technology "National Artificial Intelligence Research and Development Strategic Plan"[40] or the Commission on Civil Law Rules on Robotics for European Parliament; discussions that have taken place on an international stage. Even in India, the MeitY had constituted four committees to advice on development of a policy framework on AI. The NITI Aayog also came up with the 'AIRAWAT' approach to foster growth in the sector of AI.[41] Although, the progress is gradual, further research and dedicated action shall result in an inclusive draft policy for Artificial Intelligence that keeps pace with the technological development in the sector.

[40] Cindy Mason, 'Preparing for the Future of Artificial Intelligence - Final Report from National Science and Technology Council' (*Academia*, October 2016) <https://www.academia.edu/35544315/Preparing_For_the_Future_of_AI_Final_Report_from_National_Science_and_Technology_Council> accessed 28 January 2021

[41] Divjyot Singh, Kunal Lohani, Kumari Poorva, 'AI, Machine Learning and Big Data 2020', (*Global Legal Insights,* 21 May 2020) <https://www.globallegalinsights.com/practice-areas/ai-machine-learning-and-big-data-laws-and-regulations/india#chaptercontent6> accessed 29 January 2021

INTELLECTUAL PROPERTY RIGHTS AND SOFTWARE PATENT: A PROBLEM OF INNOVATION

Harshit Jain,[1] Anshi Mishra[2]

ABSTRACT

Intellectual property rights oblige the foundation of the software industry. The law offers different procedures for ensuring advantages of ownership subject to their sort. There are essentially four kinds of property rights appropriate to programming: patents, copyrights, trade secrets and trademarks. Each bears the expense of a specific kind of legal security. Patents, copyrights and trade secrets help guarantee the advancement itself. Trademarks protect the names or symbols used to distinguish a product within the marketplace. Both patents and copyrights are instruments that are proposed to shield an organization's or individual's advancement from maltreatment by others, notwithstanding the way that they're extremely different gadgets for doing accordingly. Copyrights, overall, guarantee the essence of an idea; copyright protection loosens up to a particular work, yet can't be applied to the musings contained in such work. The applying of copyright security for software products was steadily settled worldwide by methods for the World Trade Organization's (WTO) Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs). Under Article 10 of the TRIPs plan, WTO people are expected to treat computer programs, whether or not a thing or in source code, as creative fills in as portrayed inside the Berne Convention.

Transferring technology in an atmosphere where patent confirmation is questionable can introduce basic risks to a innovating firm's ability to appropriate rents. This paper wires lopsided information in a screening game where the growing firm has the choices of allowing one more thing at a protected distance to a new firm, conveying it, or approving it to an assistant. Subsidiary production avoids the risk of pantomime anyway incorporates more prominent costs for the propeling firm. Intellectual Property Protection for Software Innovation in software is consistently made sure about as authorized advancement, generally either through the use of copyrights or patents.

Outline of the Paper →

The paper started off with the abstract highlighting the main themes and arguments of the paper in brief just above this part of the paper. Further below is a list of sources utilised for writing this research paper for quick reference. The actual content of the research paper then begins with an introduction explaining the usage of Free and Open Source Software (FOSS) among various devices

[1] Harshit Jain, B.A. LL.B. (Hons.) 4 th Year O.P. JINDAL GLOBAL UNIVERSITY Sonipat Haryana, E-mail Address: 17jgls-hjain@jgu.edu.in
[2] B.A. LL.B. (Hons.) 4 th Year, Jagran Lakecity University, School of Law, Bhopal (M.P.)
E-mail Address: anshimishra33@gmail.com

and some proprietary entities actually seeking patent protection for their software. Post that there is a quick overview of the existing literature and observations of various scholars who have worked on the same field.

Post that, the main research begins explaining the difference between FOSS and proprietary software models. There is then a quick explanation of the requirement of innovative step for the protection of patent to be given including a brief reference to the case law *Biswanath Prasad Radhey Shyam vs Hindustan Metal Industries Ltd*[3]. The paper then refers to the problem of how innovation can be an issue in software development due to the nature of operation of the software and/or the human-readable source code.

Owing to this difficulty there is an observation made as to how India and the United States have treated software patentability on a comparative note. Also, how FOSS can actually be innovative in a practical sense is discussed. Then the paper moves on to answer the main intention of writing paper, which is, are software patents really necessary. There is no clear answer to this question, however, it is tried to be argued that some software can only be given the protection of copyright which involve a unique thought and expression, while only those software that are truly innovative in their foundation can be given patent protection. There is also a quick reference to the famous case of *Alice v CLS Bank*[4].

There is then an attempt made to classify the software into different categories (on a factual basis) and accordingly grant the right protection based on the category. The paper then ends with a conclusion explaining, in brief, the main contents and arguments of the paper while also emphasising how FOSS can be better in some ways over software patenting.

INTRODUCTION →

Free Libre and Open Source Software (FLOSS or FOSS) has been used across various machines ranging from a simple smartwatch to even supercomputers of NASA[5]. Especially with the advancement of android Operating System, the usage of FOSS is becoming widespread across various smart gadgets that we use in our everyday life. While we intertwine ourselves with various FOSS in our daily lives, there are many tech companies that are moving towards patenting their software along

[3] Biswanath Prasad Radhey Shyam vs Hindustan Metal Industries Ltd (AIR 1982 SC 1444).
[4] Alice v CLS Bank (134 S. Ct. 2347 (2014)).
[5] Sebastian Anthony, 'International Space Station switches from Windows to Linux, for improved reliability' (*Extreme Tech*, 9 May 2013), <https://www.extremetech.com/extreme/155392-international-space-station-switches-from-windows-to-linux-for-improved-reliability> accessed 11 January 2021.

with the hardware, surprisingly even those companies that use FOSS for their Operating System while claiming for Patents on their hardware invention – Xiaomi for eg. Patenting a smartphone design with in-built earbuds yet using Android as their foundational Operating System, which is a FOSS[6].

In this research paper, we will try to explore what are the difficulties that may be faced against a software patent and are those difficulties really a matter of concern for software patenting. We would also try to explore what could be a possible way ahead that can be taken to approach the issue of software patenting vs the FOSS.

Literature Review →

According to Marcus M. Dapp, ETH Zurich, innovation has been one of the major concerns of software patenting[7]. According to him, two software can do the same function as each other, however, they can be written using different source code, physically written by a human being and is readable too. However, the problem arises when we have to assess who was actually innovative because both of them write a program that gives the same output while using different logic and ideas – one person's algorithm may be better than the other which may also lead to a more efficient output of the program.

Furthermore, to elaborate on this problem precisely, Meera Jayakumar and Harsha Vardhan, has opined that the whole philosophy of the software industry is more of market-driven rather than innovation-driven – it is all about "doing it right the first time" and then claiming patent over it[8]. Jim Bessen and Bob Hunt, in their paper, *The Software Patent experiment*, concluded based on their survey that innovation has hardly been an incentive in the software industry[9].

The existing literature seems to convey the fact that software patents are not really of the nature of innovation of something new but only a race to do something first for establishing their market presence. We may slightly (though not completely) disagree with

[6] 'Xiaomi Patents a smartphone design with in-built earbuds' (*Digit*, 29 July 2020) <https://www.digit.in/news/mobile-phones/xiaomi-patents-smartphone-design-with-in-built-earbuds-55636.html> accessed 11 January 2021.

[7] Marcus M. Dapp, 'Open Source + Software Patents = Innovation? Understanding software patent policy's effects on open source innovation' (2006) <http://regulation.upf.edu/bath-06/5_Dapp.pdf> accessed 12 January 2021.

[8] Meera Jayakumar and A. Harsha Vardhan, 'Software Patents in the Indian Framework: An Economic Analysis of Problems and Prospects' [2008] NLSIR 220, 221 <https://www.jstor.org/stable/44283684> accessed 12 January 2021.

[9] Robert Hunt and James Bessen, 'The Software Patent Experiment' [2004] Federal Reserve Bank of Philadelphia, Working Paper <https://core.ac.uk/download/pdf/6648719.pdf> accessed 12 January 2021.

the way software patent is looked at as having no innovation prospects and it would be explained elaborately in the further parts of the paper.

TRIPS

The Trade Related Aspects of Intellectual Property rights was the first international treaty related computer program protection and gave different form of protections to computer program such as patents, copyrights, and trade regime. Under article 10 of TRIPS agreement it mandates the member states to protect computer program as literary work under the Berne Convention. If we read the article in more detail it meant to say that the member states have a right to choose the kind of protection of intellectual property right granted. The member states within their domestic legal system can give highest protection to software or lowest but granting of protection is mandatory. Article 27.1 of TRIPS[10] agreement states that patents should be give given to inventions in all fields of technology and that such inventions be new, have an inventive-step and are capable of industrial use. Also, Article 27.2 and 3 of the same agreement provides subject matter which are excluded from patentability by member nations. It states that for the protection of public order and morality inventions are to be excluded from patentability for commercial purposes. In brief we can understand that the agreement does not expressly provide exclusion to software programs from patentability and on the other hand the agreement also does not provide definition for terms like "invention" and "technology". In effect to this some countries exploited the gaps in the system to patents to inventions which are abstract. The U.S for instance gave patent to a system called "Virtual sales personnel"[11].

The protection granted by TRIPS agreement only focuses on the copyright protection of source code and object code, but it does not protect the valuable behavior of the program. Developers like Pamela Samson say that the true value of the software program lies within the source code and not object code[12]. In short, source code gets its value through the experience of consumer and how the software behaves. Hence, the behavior of the program should also be given protection. The TRIPS agreement till date does not provide us with the protection of pure software[13]. As such, various countries have different laws and guidelines for inventions being patented. The main issue thus arising out of TRIPS is that what kind of software is patentable and not whether software is patentable.

Main Body of the Paper →

[10]TRIPS 2003
[11]WIPO report 2003
[12]Source code is written by developer and object code is a language which is understood by computer. Object code can only be read by translating it to source code by developer.
[13](Lemley Fall 2002)

Before we decide on the legal aspects of the patentability of software programmes vs FOSS, we need to understand how to the two models differ from each other which would, in turn, help us identify the problems of Software Patenting vs FOSS. Following is the brief explanation of the two models of software explained in brief.

In the proprietary model, software are developed in a centralised, closed type of environment where the product is fully "built in house"[14]. Another important characteristic of the proprietary model is that the users are only granted licences to use the software with certain restrictions[15] - which means that the source code of the software would not be available to the user of the software. The software under the FOSS model, however, are a result of collaborative developing of people that is not restricted just to boundaries of a particular firm[16]. Under the GNU General Public Licence, the developers must not only give licence to use the FOSS but also make available the source code for any member of the community to adapt the software according to an individual's requirements.

Coming to the legal aspects of patentability, it is clear from Section 2(1)(j) of The Patents Act, 1970 (India), an invention means a product or a process involving an inventive step and capable of industrial production. We would not explore the aspect of industrial application of the software as a part of this paper and focus mainly on the innovative aspect of patentability. For applying for the patent, the applicant must be the true and first inventor of the invention according to Section 6 of the Act. While interpreting the inventive step, the Supreme Court of India has held that the test for the same must be checked in the following manner given in the case of *Biswanath Prasad Radhey Shyam vs Hindustan Metal Industries Ltd.*[17] - "Was it for practical purposes obvious to a skilled worker, in the field concerned, in the state of knowledge existing at the date of the patent to be found in the literature then available to him, that he would or should make the invention the subject of the claim concerned ?".

Moving forward to the difficulties of innovation in software, it is very difficult to actually assess the innovation aspect in software because that would convey a notion of software as a discrete product, where one product can be very different and hence an innovation compared to another. But comparing programs is difficult: new user functions

[14] Rosa Maria Ballardini, 'Proprietary Software vs FOSS' [2012] IPR UNIVERSITY CENTER 1,3 <https://ipruc.fi/wp-content/uploads/B4_Ballardini.pdf> accessed 13 January 2021.
[15] *Ibid.*
[16] *Ibid.*
[17] Biswanath Prasad Radhey Shyam vs Hindustan Metal Industries Ltd (AIR 1982 SC 1444)

may be perceived as new although the underlying source code is not new at all[18]. On a different note, two different source codes can perform the same operations which may not be perceived as something new to the users.

Owing to the difficulties of recognising innovation in software, India has ruled that software cannot itself be patented while it can be patented if it is associated with hardware and the association together has an inventive step/process involved in it. However, this idea may be problematic because definitely, one person/entity may write the algorithm and the source code of the software while the other person/entity may develop unique inventive hardware solely to run the software and may get the patent over it.

On a comparative note, in the United States, software, as is, are allowed to be patented without combining it with any specific hardware. This may pose a higher problem than the Indian scenario as finding the inventiveness or novelty in software programmes would become even more difficult as explained in the foregone paragraphs.

With FOSS, the whole source code is open to anyone that wishes to modify and adapt the software to their own requirements and give it back to the community and the process repeats with various users. Thus, innovation may also be actually happening in the form of a modification of the software - say at a certain time A, the software could do certain tasks, but with various updates and changes it may have, at time B, changed itself from the original composition of itself and thus can become a whole new invention altogether. Of course, none of the FOSS is patentable but this is just a thought.

This then brings us to the main question of the paper which is, are software patents really necessary? If not, then can we approach the method of copyrighting the source code and consider it sufficient to the protection of the Intellectual property of the software. There is definitely not a sure shot answer to the same but we would try to assess the best possible way to conclude on the same. It is clear that a patent cannot be given for a simple idea while copyright can be given to a thought and expression which is written down in a tangible media.

[18] *supra* note 3, at 9.

In the case of *Pepsi Co. Inc and Ors vs Hindustan Coca Cola Ltd. and Ors*[19], it was held that if there is a unique thought and expression conveyed through a phrase or title, that can be protected under copyright law. It was also held that copyright protection was available to the entities because they had spent an enormous amount of money for devising the unique phrase. We may see something similar happening with the proprietary entities that make software as they spend their money on devising a specific algorithm which is in turn written in a source code to develop the software. We may equate the developing of an algorithm as a unique thought because it involves a logical approach which may not be possible by everyone although someone else may approach a different logic to design a software which does the same function. Once it is written in a tangible media, it can gain all copyright reserves.

Furthermore, it may be difficult to accept that just an algorithm and logic development can be equated to a whole new innovation because it is simply a skill that a programmer can use and develop. Any man in the field can develop software based on his logical application to develop the algorithm and in turn into a human-readable source code. Thus, this can be treated as unique thought or expression that may require some protection and hence, copyright protection only might suffice the protect the intellectual property.

We may also look at a very famous US case of *Alice v. CLS Bank*[20] where it was held that merely converting an existing idea into a software cannot be treated as a patent-eligible invention – "*merely requiring generic computer implementation fails to transform [an] abstract idea into a patent-eligible invention; mere recitation of a generic computer cannot transform a patent-ineligible abstract idea into a patent-eligible matter*"[21].

To counter this point, we may notice that certain software is developed after a lot of research and development that may be an innovation in itself. Say, for example, development of Artificial Intelligence technology which is no doubt consisting only of programmes written in source code but it would be a whole new technology that may be utilised in many hardware devices. Some AI robots like Sophia, are even able to learn certain things themselves – Sophia learnt Arithmetic herself and is able to contextualise the conversations

[19] Pepsi Co. Inc and Ors vs Hindustan Coca Cola Ltd. and Ors 2003 (27) PTC 305 (Del).

[20] (134 S. Ct. 2347 (2014)).

[21] *Ibid* at 2358.

based on her past experiences and conversations[22]. This kind of software development may be truly considered as innovation because it is not a simple set of source code written and protection just under copyrights may not suffice to protect the advancement and development of such technologies.

Of course, combining with hardware, any entity can claim Patent over the hardware including the software as a whole. But in case the hardware is not yet built for the specific purposes for which the software is built, it should not be a reason to deny patent on such software because simply, the software can be used elsewhere by any other entities in their software say including it in voice assistant searches or any other applications in any device. Thus certain extremely innovative software that has been developed with research, development and in a similar manner to that of developing an innovative work can be granted patent protection to help the entity economically sustain in the market because of their true step towards an inventive process.

As we have already observed form the existing literature above that innovation has never been an important aspect with respect to the development of software as a general practice, we may agree with the same for majority software that is simply a unique thought and expression of writing a human-readable source code. However, that may not be the case always with all software as software that is similar in nature of a true innovation as has been explained above may be granted protection under patent because they are not just a unique thought and expression but whole new research and development altogether.

Classification of Software →

With that observation being made, we would move further with a certain categorisation of software that may need protection under patents or copyrights or does not need any protection at all. For convenience, we would divide all software into five broad classifications. It would be named them in the following ways.

1. Free Software – We already know what a FOSS is and any group of individuals may develop a software and obtain a license under the GNU General Public Licence. But the free software that is being tired to classify here is to mean that it must be free of

[22] 'World's first robot citizen attends conference in India; makers reveal Sophia can draw now' (*Economic Times*, 17 October 2019) <https://economictimes.indiatimes.com/magazines/panache/worlds-first-robot-citizen-attends-conference-in-india-makers-reveal-sophia-can-draw-now/articleshow/71633205.cms> accessed 11 January 2021.

any intellectual property protection rights. These software ideally have no unique thought and/or expression, let alone have any inventive step involved. If the software has such a characteristic, then it can be classified under Free Software. The software in question in *Alice vs CLS* can be one such software as it really did not involve any uniqueness in thought and the court had anyway held that it did not have an inventive step to be given protection under patent. It did not even have a uniqueness of thought and expression because it was simply turning an existing idea into a particular software.

2. Copyright Software – Those kinds of software can be classified here which may not have a substantial inventive process but somehow the algorithm used is one of a unique nature that could satisfy the requirements of protection under copyright. Most software may fall in this category because as we have learnt already from various scholars that inventive step is one of major concern in software patents. Copyright should be given to only the source code of the software and if anyone can come with a different algorithm and source code to perform the operation, then it must be allowed to do so.
3. Patent Software – These kinds of software are those which are in itself a whole research and development process rather than a mere expression of an algorithm written in source code. This may consist of multiple algorithms that are synchronised to work together or even say umpteen layers of algorithms which is very complex for any reasonable man to read the source code and understand its working and hence is not even a reasonable man's cup of tea in the industry to develop it.
4. Patent Software with Hardware – If the software as mentioned in the third category is so intertwined with any specific hardware, then both the software and the hardware can be given patent protection provided the hardware also involves an inventive step.
5. Free and Open Source Software – Enough information about this has already been given in the paper. Accordingly, any interested community of software developers can develop a software and make available its source code as well as the licence to any user. The difference between Free software and FOSS is that in Free Software, the entities can choose not to share their source code to anyone if they so wish. Otherwise, any of the four kinds of the software mentioned above, if the developers wish, can always bring it under FOSS.

Assessing what software falls into which category should be solely based on a case by case basis depending on the factual scenario.

Conclusion →

In this paper, it is being tried to argue that software patenting may not be an ideal scenario for all software developed as it severely may lack the inventive step or process as pointed out by the various scholars whose works are mentioned in the initial part of the paper. As such, granting software patents that do not truly involve an inventive step may not be a good step forward and we may have to curtail granting patents on software. In the Indian context where patents are given to a software when combined with a specific hardware, even this may need to be curtailed if the software developed does not truly involve an inventive step. Hardware patenting is a whole new topic which was not mainly the focus of this paper, however, even hardware patents must go through the same test of an inventive test to be able to grant patent protection.

For convivence, we have tried to divide the types of software based on the type of intellectual effort that is put into its development. Based on the different type of software, we can choose the different type of protection that can be given.

Free and Open-Source Software on the other hand has many advantages over the idea of innovation. Although some scholars may argue that due to budgetary restrictions, the implementation of innovation in FOSS can be problematic, it is also noteworthy that freedom to alter the source code as per the requirements of the individual can be an indirect innovation that may lead to benefit of many users. Thus this can also take an industrial application which is why Android OS, which is a FOSS, has been so widespread in the manufacture of smart gadgets from the last decade. Apart from this, FOSS also has the benefit of security as anyone can update the security packets of the source code if they find any fault and the user may not really wait till an entity actually recognises and fixes it.

While the debate upon patenting software vs FOSS has been the talk of the era, there has been an approach towards a hybrid model of software where some of the source code is taken from the FOSS and some of it is written by the proprietary entity. This has been a recent developing trend in the software industry which has its own pros and cons and requires another detailed study. Interested candidates may pursue the same and analyse the intellectual

property protection rights of such software and see if they can classify those in the classifications mentioned in this paper or maybe add another classification assessing its patentability or copyright protection.

FIXING LIABILITY FOR AUTOMATED VEHICLE AND PROTECTING INNOVATIVE AUTOMOBILE TECHNOLOGY IN INDIA

Sahana R,[1] Olivia De,[2]

ABSTRACT:

With the advent of automated vehicle technology, the prospect of improved traffic control, increased safety, reduced carbon emissions, decreased number of accidents along with enhanced productivity has been introduced. While the amendment to the Vienna Convention on Road Traffic, in the year 2014, allowed manufacturers to develop and make automated vehicles further opening up a greater opportunity in the automobile industry, it however at the same time has increased the liability and environmental risks arising out of the operation of such vehicles. The Motor Vehicles Act' 1988 in India by failing to mention authorisation of self-driving vehicles to be manufactured, sold or driven in the country, serves as a disincentive for start-ups, FDIs and Make in India campaign. Introducing an inclusive law will encourage indigenous companies to innovate and receive protection for such technology inturn escalating the economy. The revolution in automobile technology will be a challenge in the absence of precedents or legal framework while fixing liability and accountability. Certain developed countries such as the United States, United Kingdom, Australia, Canada, etc have sanctioned the growth of this technology while attempting to curb the risks through various legislations and policies. This paper is a non-empirical study that first introduces the different issues related to automated vehicles by studying the legal advancement in other countries and analyses the status of automated vehicles in India. It then explores the chilling effect of liability and the issue relating to protection of innovations by start-up manufacturers of automated cars in India.

Introduction

"Exploration is the engine that drives innovation. Innovation drives economic growth."- Edith Widder

According to WHO's report, road traffic accidents are predicted to surpass cancer and HIV/AIDS related deaths to become the fifth leading cause of death by 2030.[3] According to the Eno Center for Transportation's 2013 report, just by converting 10% of the U.S. vehicle to automated cars, each year the number of accidents will reduce by 211,000.[4] However, road crashes will never become zero with usage of Automated vehicles since in 2016, a Tesla operating AV in Florida met with an accident killing the Tesla's driver, when it crashed into a tractor-trailer which had made a left turn in front of

[1] School of Law, Student, Christ University Email Address- sahana3ravi@gmail.com
[2] School of Law, Student, Christ University Email Address- payel.olivia2001@gmail.com
[3]WORLD HEALTH ORGANISATION, *Injuries and Violence: The Facts* 2014 <https://www.who.int/violence_injury_prevention/key_facts/VIP_key_facts.pdf > accessed 28 November 2020.
[4] ENO CENTRE FOR TRANSPORTATION, *Preparing a Nation for Autonomous Vehicles* (2013) 8 <https://www.caee.utexas.edu/prof/kockelman/public_html/ENOReport_BCAofAVs.pdf > accessed 5 January 2021.

the vehicle.[5] Another accident in 2016 by an AV was reported wherein a Google automated car miscalculated that a public bus would slow down and let the car to converge, however the bus proceeded and got sideswiped by the car.[6] The road crashes in India are generally on account of driving in a drowsy state or under the influence. The revolution in the automotive industry is identified by introducing self-driving vehicles which is predicted to reduce road fatalities, ease traffic congestions, help reach destinations quicker and decrease emissions since the in-built computerised systems can maintain steady cruising speed along with choosing the most economic fuel route.[7] However, it is also predicted on the contrary that energy consumption might increase by upto 200%[8] with convenient and easy automated driving facilities. The Union minister for Road Transport and Highways Minister in 2017 stated that autonomous vehicles will be disallowed in India since such driverless technology will arrest the employment and livelihood of millions.[9] In the backdrop of no legal framework allowing automated vehicles or safeguarding the drivers of self-driving cars since the 2019 Amendment to the Motor Vehicles Act' 1988 failed to include any provision relating to automated vehicles in India, it has served as a disincentive for automated car manufacturers to enter the Indian market thereby affecting the economy. While the presence of poor road infrastructure with narrow lanes at places or uneven roads have obstructed the market players, it hasn't entirely made them retreat back. In the 2016 Defexpo held in Delhi, a driverless shuttle, Novus Drive was the first automated vehicle to debut in India, being indigenously manufactured and 100% eco-friendly, it was lauded by Union Transport Minister Nitin Gadkari.[10] Driverless vehicles are no longer a distant dream in India with Tesla, the leading self-driving tech giant, announcing the launch of its automatic model in 2021[11] in India and registering it soffice in Bangalore.[12] Automotive is the fastest growing area in the 31 billion dollars Indian R&D space.[13]

---

[5] Bill Vlasic and Neal E., 'Self-Driving Tesla Was Involved in Fatal Crash, U.S. Says' THE *NEWYORK TIMES (*30 June 2016) <https://www.nytimes.com/2016/07/01/business/self-driving-tesla-fatal-crash-investigation.html > accessed 12 January 2021.

[6] *Joseph Serna*, 'Video Shows Google Self-Driving Car Hit a Bus in Silicon Valley' *L.A. TIMES* (9 March 2016), <https://www.latimes.com/local/lanow/la-me-ln-video-google-car-20160309-story.html > accessed 15 January 2021.

[7] Payton Chang, 'Self-Driving Cars and Their Environmental Impact' 2017 STANFORD UNIVERSITY <http://large.stanford.edu/courses/2017/ph240/chang-p2/#:~:text=Pros%20of%20Self%2DDriving%20Vehicles&text=Vehicles%20will%20then%20be%20lighter,the%20most%20fuel%20efficient%20route> accessed 8 January 2021.

[8] J. Worland, 'Self-Driving Cars Could Help Save the Environment Or Ruin It. It Depends on Us' *Time (*16 September 16 2016) < https://time.com/4476614/self-driving-cars-environment/> accessed 2 January 2021.

[9] Dipak K Dash, 'Driverless tech will leave millions without jobs, won't allow it: Gadkari' *The Times of India (*25 July 2017) <https://timesofindia.indiatimes.com/auto/cars/government-wont-allow-driverless-cars-on-indian-roads-nitin-gadkari/articleshow/59741458.cms > accessed 18 December 2020.

[10] MotorIndia, 'THRSL receives huge applause for Novus-drive, the driverless vehicle' *MOTORINDIA* (15 February 2016) <https://www.motorindiaonline.in/applications/hi-tech-demonstrates-driverless-vehicle-capability-with-novus-drive/> accessed 17 December 2020.

[11] HT Auto Desk, 'Tata to Tesla: Electric cars expected to launch in India in 2021' *HINDUSTANTIMES* (11 January 2021) <https://auto.hindustantimes.com/auto/cars/tata-to-tesla-electric-cars-expected-to-launch-in-india-in-2021-41610361859908.html> accessed 14 January 2021.

The United Nations Economic Commission for Europe (UNECE), set up in the year 1947, made a regulatory amendment in 2016 to the Vienna Convention on Road Traffic 1968 allowing automated vehicle technology to be deployed on the roads provided that all the safety standards were in conformity with the United Nations Vehicle Regulations.[14] Through the UN Regulation No 79, the speed limit of 10 kilometer per hour was removed. This was a milestone in technology building and regulation of such technology.[15] The UNECE has been a compelling force in increasing the progress in the field of autonomous vehicle technology. Therefore, under the guidance of the UNECE, a Working Party on Automated/Autonomous and Connected Vehicles was set up in the year 2018. Various countries such as Korea, Japan, the United States of America and many more cooperated with the Working party by offering expertise in Automobile technology.[16]

The Time Magazine in its March 2016 cover titled "No traffic. No accidents. No deaths. All you have to do is give up your right to drive" featured automated cars.[17] The requirement of automated vehicles in India has its pros and cons. While on one hand, the automated vehicles bring down the risk of drunken driving to a great extent, promotes growth of innovation in the country, and eases the activity of driving, on the other, the automated vehicles are not suitable for Indian roads with the associated invasion of privacy issues and unaccounted liability arising out of automated vehicle accidents. This paper shall analyse these pros and cons and how regulating automated vehicles in India can prove to be beneficial by minimising risks.

Global Legal Response to Automated Vehicles:

The various policies, regulations and enactments through which various developed countries like Australia, Canada, United Kingdom, United States of America have welcomed the automated

---

[12] Shilpa phadnis,Chetan kumar and Avik Das, 'Tesla drives into Bengaluru with new company*' THE TIMES OF INDIA* (13 January 2021) <https://timesofindia.indiatimes.com/city/bengaluru/tesla-drives-into-bluru-with-new-co/articleshow/80239716.cms> accessed 15 January 2021.

[13] Shilpa phadnis,Chetan kumar and Avik Das, 'Tesla drives into Bengaluru with new company*' THE TIMES OF INDIA* (13 January 2021) <https://timesofindia.indiatimes.com/city/bengaluru/tesla-drives-into-bluru-with-new-co/articleshow/80239716.cms> accessed 15 January 2021.

[14] United Nations Economic Commission for Europe, *UNECE paves the way for automated driving by updating UN international convention* (23 March 2016) <https://unece.org/press/unece-paves-way-automated-driving-updating-un-international-convention#:~:text=UNECE%20paves%20the%20way%20for%20automated%20driving%20by%20updating%20UN%20international%20convention,-23%20March%202016&text=A%20major%20regulatory%20milestone%20towards,Vienna%20Convention%20on%20Road%20Traffic> accessed 3 January 2021.

[15]The United Nations Economic Commission for Europe, *Uniform provisions concerning the approval of vehicles with regard to steering equipment* (2005 Regulation Number 79, Addendum 78) 25.

[16]United Nations Economic Commission for Europe, *Driving Progress on autonomous Vehicles* <https://unece.org/DAM/trans/doc/2019/wp29grva/Autonomous_driving_UNECE.pdf > accessed 12 January 2021.

[17] Matt Vella, 'Why You Shouldn't Be Allowed To Drive*' TIME* (7 March 2016), <https://time.com/magazine/us/4236955/march-7th-2016-vol-187-no-8-u-s/ > accessed 2 December 2020.

vehicles and regulated such vehicles to get the first mover's advantage and act as a stimulus for car manufacturers, are as follows:

United Kingdom

The Government's aim to globally embrace and catalyse the growth of automated vehicles was met when in 2018, the Automated and Electric Vehicles Act' 2018 (AEV Act) received the Royal Assent along with setting up of a separate department, Centre for Connected and Autonomous Vehicles, for this purpose. From an insurance point of view, this statute is one step ahead since it addresses all possibilities arising out of a claim for an accident. While the insurers are liable to pay if the vehicle was in self-driving mode and the driver sustained injuries, the insurer can seek a claim from the manufacturers if it is ascertained that a manufacturing defect was the cause of the damage. However, the insurers are free from liability or have limited liability if it is established that the insuree made or failed to make certain software alterations mandated under the insurance policy.[18] The much debated 'user liability' concept was settled in December' 2020 when the Law Commission recommended that the manufacturer or developer of the car should be liable instead of the driver if the vehicle is in self-driving mode.[19]

United States of America

In the United States of America, the Department of Transportation has undertaken an Automated Vehicles Comprehensive plan to prepare a safety net around the future automobile technology. This plan aims to promote transparency, collaboration and create a regulated environment for all automated vehicles within the country.[20] The Federal Automated Vehicle Policy of 2016 provides certain guidance to the manufacturers as well as the drivers of automated vehicles for safe deployment of autonomous vehicles.[21] The National Highway Traffic Safety Administration (NHTSA) identified five levels of Automated Driving systems that are Level 0 with no automation, Level 1 with driver assistance, Level 2 is partial automation that includes combined automated functions, Level 3 is conditional automation, Level 4 is high automation and Level 5 is Full automation. The Federal policy states that the manufacturers must follow a model state policy and not

[18] Steven Baker, 'How UK law is adapting to cope with Autonomous vehicles' *Engineering and Technology* (27 May 2020) <https://eandt.theiet.org/content/articles/2020/05/how-uk-law-is-adapting-to-cope-with-autonomous-vehicles/> accessed 20 December 2020.

[19] Martin Stanley, 'Understanding Regulation- Autonomous Vehicles' Regulation.org, <https://www.regulation.org.uk/specifics-autonomous_vehicles.html#:~:text=The%20government%20announced%20in%20November,was%20involved%20in%20a%20collision> accessed 29 December 2020.

[20] U.S. Department of Transportation, 'Automated Vehicles Comprehensive plan' (January 2021), <https://www.transportation.gov/sites/dot.gov/files/2021-01/USDOT_AVCP.pdf> accessed 30 January 2021.

[21] U.S. Department of Transport, *Federal Automated Vehicles Policy: Accelerating the Next Revolution In Road Safety*, 12507-091216-v9 2016 NHTSA <https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf> accessed 29 December 2020.

make vehicles differently for different states. The model state policy was to be formed by engaging with the stakeholders and conducting public workshops. The National Highway Traffic Safety Administration would be the regulatory board, regulating all the Automated vehicles in the country. The estimation by the National Highway Traffic Safety Administration (NHTSA), presently even developing standards for V2V communication, is that such technology can reduce all accidents by 81%.[22] In the United States, twenty-nine states have enacted a legislation to regulate autonomous vehicles within the state. Some of the states are California, Florida, Illinois, Oregon, Indiana, Louisiana, North Carolina, Maine, New York, Michigan, Nevada, Mississippi, and so on.

Fixing Liability

The automated vehicle technology opens up a sphere of driving with benefits and reduces the risks associated with driving. However, risks of automated driving will not become nil since there are probabilities of accidents by self-driving vehicles. These risks can only be reduced to an extent through regulations but cannot be negated to its entirety. Therefore, when such accidents take place, the question of who is liable for the accident if the vehicle was self-driven arises. Another question that arises is whether the accident happened due to the negligence of the driver or manufacturer. With the unprecedented development of AV, the magnitude of risks associated increases by several folds. Arguably, companies like General Motors, Cruise and Waymo had introduced AV's without pedals or a steering wheel[23] thereby completely snatching any control which can be exercised by a driver.

Connecting automated vehicles to a negligence standard will result in an improved outcome by reducing crashes apart from accelerating the adoption of automation.[24] In general, fixing liability on the manufacturer sounds practical given that the vehicle instead of the driver is in control of the car in self-driving mode and the manufacturers are responsible for software and safety of the vehicle. However, there has never been an obligation on a manufacturer "to design a fool-proof or accident-proof vehicle."[25] Even from an economic perspective, transferring liability to the manufacturers is feasible since they are the least cost avoider i.e. the party which can reduce negative externalities efficiently by increasing safety standards. However, this assignment of liability is linked with exploitment of manufacturers. Victim-plaintiffs will reap unethical benefits out of such default liability rule and it will serve as a disincentive to the major market players as well as start-up

[22] J. Harding, 'Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application' 2014 report no. DOT HS 812 014, US Nat'l Highway Traffic Safety Administration <http://bit.ly/2jC4O0V> accessed 5 January 2021.
[23] Timothy B. Lee, 'Congress debates allowing tens of thousands of cars with no steering wheel' *ARS Technica (*16 March 2018) <https://arstechnica.com/cars/2018/03/congress-debates-allowing-tens-of-thousands-of-cars-with-no-steering-wheel/> accessed 12 February 2021.
[24] Ryan Abbott, The Reasonable Computer: Disrupting the Paradigm of Tort Liability, 86 Geo. Wash. L. Rev. 1 22 (2018).
[25] Larsen v. Gen. Motors Corp., 391 F.2d 495, 502 (8th Cir. 1968).

manufacturers. Furthermore, the litigation costs arising out of such liability standard might shift to consumers in the form of increased price or push the smaller market players out of the market. A solution can be found by affixing liability on either parties according to the part played in the accident. For instance, if the AV jumps a traffic signal or misunderstands the speed of a vehicle being overtaken or fails to identify an object or individual on the road, the liability can be fixed on the manufacturer as the direct cause of accident was the malfunction of the software, the reasonable care of which was the duty of the manufacturer. However, in instances where the driver of the vehicle was completely at fault without any failure in the automated technology, the manufacturer cannot be held liable and imposed costs upon. Complicated situations arise wherein the accident occurs while the driver was simultaneously switching between self-driving and manual driving options. In such scenarios, while fixing liability, the driving mode should be looked at. If for the last couple of minutes the vehicle was in automated mode and the software malfunctioned beyond the control of the driver, the driver will not be liable.

While driving, whether an automated vehicle or manual vehicle, the driver must take utmost care and operate in such a manner which is within the driver's control. If an accident was beyond the reasonable control and operation of the driver it would not constitute a negligent act. However, in every incidence involving a motor vehicle accident, the driver's negligence must be proven. The Apex Court in *Minu B. Mehta v. Balkrishna Ramchandra Nayan*[26] held that the liability would not arise unless a person contravenes any of the common law or other statutory duties imposed upon him in a motor vehicle's accident case. The court subsequently further held that if such a contravention of the duties of a driver occurs, the owner of the vehicle will be made vicariously liable to pay compensation. Generally, in the case of an automated vehicle which is self- driven and involves no negligent contribution of the driver in the accident, he may not be held liable for his acts. If an accident takes place when the driver is driving the vehicle in manual mode, it would either be the driver's liability or the owner of the vehicle would be vicariously liable.

Section 140 of the Motor Vehicles Act' 1988 deals with no fault liability. In extreme cases of death or permanent disability of the victim, even with no negligence on the part of the driver or manufacturer, the party shall be liable to pay damages to the victim of the accident. In *Gujarat State Road Transport Corporation, Ahmedabad v. Ramanbhai Prabhatbhai and Anr,*[27] the Apex court observed the rising accidents caused by motor vehicles and stated that these motor vehicles are within the principle of Strict liability as held in *Ryland v Fletcher*[28]. In an accident relating to an automated

[26] Minu B. Mehta v. Balkrishna Ramchandra Nayan, 1977 AIR 1248 (India).
[27] Gujarat State Road Transport Corporation, Ahmedabad v. Ramanbhai Prabhatbhai and Anr, 1987 (3) S.C.C. 234 (India).
[28] Ryland v. Fletcher, [1868] UKHL 1 (United Kingdom).

vehicle, there may be no fault of any party in the accident but the drivers of automated vehicles are strictly liable. The justification for this form of liability is that actors participating in extremely uncommon activities are more conscious of the risks involved in such an action and should thus bear the associated costs, irrespective of whether they are legally liable for the accident.[29] No fault liability when coupled with a comprehensive federal regulatory regime can speed up the utilization and development of this technology.[30]

Safeguarding Innovation by Start-up Companies

Facilitating the Made in India campaign, the start-up industry has started being involved in the automated vehicle industry with Flux Auto, a Bangalore based driverless truck startup promoting better efficiency and cruise control with decreased accidents; Fisheyebox, a tech startup based out of Kolkata making affordable automated vehicles run by joystick; Hi Tech Robotic Systemz, a Gurgaon based startup which launched Novus-Drive and utilises Cloud Based Intelligence for fleet management system; ATImotors, a Bangalore based startup manufacturing autonomous electric cargo vehicles, with a major focus exporting out of India; Netradyne, based out of Bengaluru and San Diego, manufactures an intelligent camera that studies driving patterns and determines the cause of an accident; Swaayatt robots, a startup by an IIT Roorkee alumnus focuses on easing the handling of unseen environments by producing high speed trajectories in bestrewed environments uncovered by GPS navigation present being used in Mahindra Bolero for testing purposes; Auro Robotics, startup by IIT Kharagpur alumni producing autonomous shuttle by relying heavily on LIDAR technology, is presently being tested in the University of Santa Clara; OmniPresent Robot, a leading provider of robotics in India is utilising 3D maps and testing deployment of monocular camera for decoding road signs and detecting traffic lights; SeDriCa 1.0, by IIT Bombay's Innovation Cell, reached up the fourth spot globally in the 2016 Intelligent Ground Vehicle Competition (IGVC).[31]

Establishing and executing a comprehensive IP strategy can play a crucial role in the success of both the technology startup and the automotive supplier since that allows the company to identify and protect its IP, while being able to retain the ownership of the IP.[32] Innovative ideas and new

[29] Anderson, James M., Nidhi Kalra, Karlyn D. Stanley, Paul Sorensen, Constantine Samaras, and Oluwatobi A. Oluwatola. "Liability Implications of Autonomous Vehicle Technology." In *Autonomous Vehicle Technology: A Guide for Policymakers*, 111-34. RAND Corporation, 2014. <http://www.jstor.org/stable/10.7249/j.ctt5hhwgz.14.>Accessed January 13, 2021.

[30] Anderson, James M., Nidhi Kalra, Karlyn D. Stanley, Paul Sorensen, Constantine Samaras, and Oluwatobi A. Oluwatola. "Liability Implications of Autonomous Vehicle Technology." In *Autonomous Vehicle Technology: A Guide for Policymakers*, 111-34. RAND Corporation, 2014. <http://www.jstor.org/stable/10.7249/j.ctt5hhwgz.14.>Accessed January 13, 2021.

[31] Deoras S, "9 Startups in India Working on Self Driving Technology" (*Analytics India Magazine*February 5, 2020) <https://analyticsindiamag.com/9-startups-india-working-self-driving-technology/> accessed January 10, 2021

[32] Srinivasa CK, "Intellectual Property Considerations For Autonomous Vehicle Technology Startups And Automotive Suppliers - Technology - United States" (*Mondaq,* January 30, 2019)

technologies developed by the various companies which are protected by Intellectual Property stand a greater chance in the market. Acquiring intellectual property in innovative technology and retaining such ownership influences the decisions of third parties such as consumers, investors, shareholders, etc.[33] Protecting innovative technology designed by startups boosts the economy by serving the Make in India campaign and marketing it significantly without any obstruction by the competitors. Although obtaining a patent is an expensive and time-consuming process, it provides the exclusive right to make, use or sell an invention thus excluding the competitors from making or selling the patented invention.[34] However, startups should conduct a patent search to ascertain that their business is free of patents that other companies own in order to avoid assertion by those companies against their product or service.[35]The invention must be patentable and not fall under the realm of Section 3 of the Patent Act' 1970.[36] Furthermore, the technology to be patented should meet the essentials of being innovative and having efficacy.[37] Therefore, the automated vehicle technology created by each company must be significantly original and new to be granted a patent.

Since the automobile industry is developing at a rather fast pace and the revolution in automated vehicles has expanded the scope of this industry, there are few challenges that such an industry poses on Intellectual Property Rights. As the technology is evolving expeditiously, some businesses may have intellectual property and therefore increase the technology licensing required by other companies. Start-ups may have to invest a lot of capital and energy in Research and Development of the technology to protect it with Intellectual Property. Though, with the growth of technology, Intellectual Property challenges increase, however at the same time, the economy and market grows.

Conclusion

Being the future of automobile technology in the world, the research and development in the Automobile sector has increased and the entry of automated vehicles is inevitable, with Tesla opening their office in Bangalore apart from the presence of various automated vehicle startups in India. In order to allow the automated vehicles to enter the market, the Government must regulate the manufacturing and setting a safety test standard for these vehicles by enforcing policies, enactments

<https://www.mondaq.com/unitedstates/Technology/776022/Intellectual-Property-Considerations-For-Autonomous-Vehicle-Technology-Startups-And-Automotive-Suppliers> accessed January 12, 2021

[33] "IP & Business: Intellectual Property, Innovation and New Product Development" (July 2005) <https://www.wipo.int/wipo_magazine/en/2005/04/article_0002.html> accessed January 12, 2021

[34] "What Start-Ups Need to Know About Intellectual Property" (*The National Law Review*) <https://www.natlawreview.com/article/what-start-ups-need-to-know-about-intellectual-property> accessed January 13, 2021

[35] "What Start-Ups Need to Know About Intellectual Property" (*The National Law Review*) <https://www.natlawreview.com/article/what-start-ups-need-to-know-about-intellectual-property> accessed January 13, 2021

[36] Patent Act 1970, s. 3

[37] Novartis Ag v. Union Of India & Ors, AIR 2013 SC 1311 (India)

etc. The insertion of Section 2B, through the 2019 Amendment to the Motors Vehicle Act, provides the government the option to exempt innovations, new technologies and inventions in the form of vehicles from being subject to the provisions of the MV Act in order to promote such innovations and technologies. At the same time, to encourage more inventions in the Artificial intelligence and Automobile sector, the government can grant subsidies in patent application. The law has the power to either incentivise or curb innovation.[38] Excessive unwarranted regulation can create a chilling effect[39] on innovation and invention as apart from discouraging new players from entering the automotive industry, it can also create hurdles for the existing players who may find complying with the regulatory requirements challenging.[40]

By analysing the National Highway Traffic Safety Administration (NHTSA) and the National Transportation Safety Board (NTSB) reports, it can be concluded that probable causes of fatal crashes span from human driver's inattentiveness to driving environment complexity,[41] ignorant attitude towards the take-over request from the vehicle,[42] and distraction from some secondary tasks[43]. In India, the road infrastructure and behaviour of consumers requires a legal framework which is different from other countries. The AV might fail in narrow roads, or uneven kutcha roads, or in crowded market areas or in areas with cattle presence or other scenarios. A law should be designed to mandate maximum speed limit for AV's depending on the road infrastructure, for instance, maximum 20 kmph in crowded area or kutcha road and maximum 80 kmph in National Highways. In Tesla's models, an acknowledgement box shows up when a driver enables the auto-pilot system, indicating that autopilot mode is just a support mechanism that allows the driver to hold on to the steering wheel at all times."[44] The law should mandate availability of autopilot as well as manual driving mode along with associating 'volenti non fit injuria' to the operator of the vehicle in cases where the driver doesn't follow the pop-up. Most accidents in India happen when truck drivers drive at night under

[38] Nishith Desai Associates, 'Preparing for a Driverless Future' (May 2019) <http://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research%20Papers/Preparing_For_a_Driverless_Future.pdf> accessed 10 January 2021.

[39] Saahil Dama, 'Dear Mr Gadkari, Why So Passive Towards Autonomous Vehicles?' *THE QUINT* (2 April 2018), <https://www.thequint.com/tech-and-auto/open-letter-to-nitin-gadkari-on-autonomous-vehicles-for-india> accessed 10 January 2021.

[40] Satish N. and Ors. v. State of Karnataka, ILR 2017 Kar 735 (India).

[41] DOT-National Highway Traffic Safety Administration (NHTSA), *Office of Detective Investigation-Preliminary Report Summary 2015 Tesla Model S Crash* (January 2017) PE 16-007 (ODI Resume) <https://static.nhtsa.gov/odi/inv/2016/INCLA-PE16007-7876.PDF> accessed 12 November 2020.

[42] "NTSB News Release National Transportation Safety Board Office of Safety Recommendations and Communications" (*National Transportation Safety Board (NTSB)* <https://www.ntsb.gov/news/press-releases/Pages/nr20180607.aspx> accessed 13 February 2021.

[43] "Accident Report Detail" (*National Transportation Safety Board (NTSB)* <https://www.ntsb.gov/investigations/AccidentReports/Pages/HWY18MH010-prelim.aspx> accessed 1 January 2021.

[44] Vlasic B and Boudette NE, 'Self-Driving Tesla Was Involved in Fatal Crash, U.S. Says' *The New York Times (*30 June 2016) <https://www.nytimes.com/2016/07/01/business/self-driving-tesla-fatal-crash-investigation.html> accessed 10 January 2021.

influence or under tiredness and fatigue. The Automated Vehicle can guide the tired driver upto a limit, however, they should at all times be aware of the surroundings and switch to manual mode if the software misinterprets or malfunctions by a little. The AVs can't be used as an excuse for accidents occuring while driving under influence and they should be penalised in the same way they are being penalised at present.

In the backdrop of no ascertainment on the liability aspect for automated vehicle accidents by any statute and the customer's hesitance to purchase such a car, Daimler AG, Mercedes-Volvo and Benz's Google have all vowed to take responsibility in the case of an accident caused by their automated vehicles. To protect consumers against design defects, manufacturing defects, failure to warn, unfair trade practices, misrepresentation, negligence, breach of warranty and strict liability, the Consumer Protection Act of 2019 comes to aid.[45] According to MIT's Computer Science and AI Laboratory's Ramya Ramakrishnan, the development of the latest paradigm which utilises human inputs to discover 'blind spots' of artificial intelligence in automated vehicles to prevent accidents or mistakes in the actual world.[46] To become a powerful world economy in the 21st century, an appropriate legislation which promotes and regulates automated vehicles is required to keep up with the global driverless revolution.[47]

[45] Nishith Desai Associates, 'Preparing for a Driverless Future' (May 2019), <http://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research%20Papers/Preparing_For_a_Driverless_Future.pdf> accessed 10 January 2021.

[46] Abhinav Jakhar, 'Indian Origin Team Develops Model for Safer Self-driving Cars' *NEWS18* (28 January 2019) < https://www.news18.com/news/auto/indian-originteam-develops-model-for-safer-self-driving-cars-2016321.html> accessed 10 January 2021.

[47] Nishith Desai Associates, 'Preparing for a Driverless Future' (May 2019), <http://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research%20Papers/Preparing_For_a_Driverless_Future.pdf> accessed 10 January 2021

SMART Laws for SMART Society and SMART Technologies: Need of the Hour

Ms. A. Raja Rajeswari[1]

ABSTRACT:

SMART is the new benchmark of evaluating the standard of living of people. Where usage of televisions, ACs and Cars were always determinant factors of ascertaining the living conditions of people, today what adds value to these machines is their ability to interact with other devices in a SMART way. Internet of Things (IOT) and Artificial Intelligence (AI) have paved their way to everyday lives of people through 'Smart phones', 'Alexa', 'Home Security systems' and even 'Smart toys'. But the major concern in this interface between humans and technology is the ability to derive certain data from certain patterns of activities of humans and its interpretation for certain purposes by some private entities or even government at large. Indubitably, because of the different kinds of solutions that can be provided by IOT/AI the issue of data protection does not stand as a hindrance to its adoption. Nevertheless, addressing data protection issues is important because:

- Data protection is an important aspect of privacy, which is a fundamental right of an individual.
- Data protection laws mandating in-built security would instil confidence in people at large.
- Smart-Cities concept cannot be fulfilled without acceptance from public at large.

The IT Act 2000 addresses many aspects of cyber security and surveillance that may be applied to IOT and AI oriented SMART devices. With the introduction of the Data Protection Bill, 2019 this aspect of data protection gains much more momentum. The paper is an attempt to study the effectiveness of the existing laws in balancing the technological innovation and protection of personal data, whether the new Bill strengthens the individual's right or Right to Information and also to identify the issues of various stakeholders including service providers, consumers and Government.

Law and Technology:

Today we live in an era where we can witness certain 'things' which could only have been imagined in an advanced science fiction book or in mythological stories by a god or a person possessing such powers. The imagination of a man has met scientific advancements

[1] Assistant Professor, ICFAI Law School, Hyderabad.rajarajeswari@ifheindia.org

like ‘Internet of Things’ (IOT) or ‘Artificial Intelligence’ (AI), where the things surrounding us, like a traffic signal or any normal electronic item at home or workplace, may be used for generating certain data in addition to its normal functions through certain sensors and wi-fi. So, the physical things may interact with virtual technology and produce an outcome in accordance with a specific command(s). In the new era of connected world, people are now equally part of the integration and knowingly or unknowingly interact with physical and virtual things through the internet. One does not have to share one’s preferences or disclose information about his location and movement. All these are capable of being extracted through this conglomeration of various things surrounding us.

No doubt, in our personal space we voluntarily set the commands for the things. But when the technology is applied in a larger scale people have limited role to understand the various data that may be collected by the devices even if they are informed about its existence. The major concern in this interface between humans and technology is the ability to derive certain data from certain patterns of activities of humans and its interpretation for certain purposes by some private entities or even government at large. When movements of an individual are continuously monitored and stored for certain time, the information to an individual of such surveillance is not enough. What is even more crucial is the aspect of safety of such data stored and protection of such data from any third-party intruders. With so many devices connected into a mainstream function, even if one device leaves gap for the hackers, the security of the data and its privacy would be at stake.

For example, many of the latest technological innovations are based on IOT, where every connected device is capable of sending and receiving information that may provide valuable data to both the user, service provider or even to hackers in case of weak security encryptions. Who could have imagined a fish tank to be a source for stealing data from a Casino? Yes, it was possible through the way it was connected to internet for adjusting the temperature and salinity of the tank. there are many cases where this kind of unauthorized access could have been prevented with better equipped security measures or with timely interventions. The Chinese Company, Orvibo’s failure of security in its smart home device clearly exemplifies this.

IOT is a massive technology not only in terms of its application and uses but also in terms of its functionality. The way simple things are used as starting points for gathering data and

how through various means this data is exchanged through a streamlining process is very interesting as well as challenging from the security concerns. In technological terms the whole process may be divided into the following stages:

1. Devices: This is the first stage where a device meets the actual environment from which information is extracted. The device is usually composed of sensors or actuators.
2. Processing: This is the second stage where certain Gateways are used to process the input data into digital data for further usage and interpretation.
3. Application: This is where data is changed into database for large-scale storage. These are referred to as Data Centers and Clouds where large amount of data may be analyzed and stored. (Data Governance)

Identifying and fixing security concerns in IOT is a mammoth task. This is particularly true because of the various kinds of devices that can be used in the process and no particular security measure would be suitable for all those different devices. IOT is not used exclusively in most cases but is sometimes accompanied by other technology like Artificial Intelligence, as in the case of Facial Recognition Bot.

In India, too, SBI's lack of diligence by not protecting one of its servers with password led to data leakage of account numbers, phone numbers and account balance information.

Right to Privacy:

Privacy, which has now been accepted as fundamental Right, began to be recognized through minority or dissenting opinions whether it was through K Subba Rao, J (as he was then) in the year 1963 in India or by Justice Louis Brandeis in1928 in the landmark US judgment in which the majority refused to hold that wiretapping by government officials violates the 4th Amendment Constitutional Rights. Overall, it must be accepted that world-over, even in countries like France and Germany which recognized Privacy rights, the essence of its domain developed through the case laws itself.

Privacy intrusions may be physical in nature, for example restricting the movement of a person unjustifiably. It can be psychological as in the case lie detectors used without consent of accused. Privacy intrusions can also be by the data surveillance. This third form of privacy invasion in what is becoming more challenging, especially in this technology-oriented era. The culture of online storage of data is not anymore, a personal choice. Here again the government plays a prominent role by imposing a digital culture. The digital culture

binds the society together so intricately that the gateway between personal-private space and public life becomes blur. The right of private space is not just an elitist luxury but a common comfort of all humans wherein they can fearlessly conduct their activities in public life. It is about exercise of one's choice, whether to disclose their information or not. It is about the individual's right to determine whether certain intrusion would affect their privacy or not. For that matter, even criminal law respects this choice by not considering self-incriminating evidence, though the purpose is to protect him from coercion or undue influence. The right to be not unnecessarily dragged into public space and the rights preventing others from getting undue benefit of another's private space is a basic requirement of a civil society. In an urge to grow modern, the essential structure of a civil society cannot be hampered. Where promise of an efficient future undermines the social fabric of the society itself, there is a great probability of disturbance to the socio-psycho factors in individuals as well as economic-political factors of the nation at large. It is for this reason that Privacy is recognized as a Natural Right inherent in a human being, a right that weighs above other rights provided by the State. A Natural Right ought to be protected by a State at any cost.

It was rightly stated in Gobind V State of Madhya Pradesh that 'Privacy is a pre-condition for the enjoyment of other Fundamental Rights'. Privacy is not merely about a private space; it is to have dignity in the public sphere. When every kind of information can be obtained by IOT technology, it is very important to understand what kind of information is being processed and whether there are any filters while this information is transmitted completely or partially and who all can have access to such filtered/unfiltered information. That information may be very crucial for a person's dignity, an underpinning requirement for life and personal liberty. Thus, even informational privacy is equally important because as the court observed that 'an individual cannot be left to an unregulated marketplace.

In Europe, Privacy and protection of personal data is recognized by the EU Charter of Fundamental Rights. Under Article 8 of the Charter every person has a right for protection, access, and rectification of collected data. The EU's GDPR, which came into force on 25th May 2018, is not just a reflection of people's right to same data protection rights irrespective of where it is processed, but also an effective way of ensuring 'single digital market' providing an easy platform for free flow of data across Europe.

In similar lines, India has initiated its efforts for a data protection law. Here again the dissenting opinion of Y.V. Chandrachud, J, becomes relevant as despite not accepting

Aadhaar as being not violative of privacy rights, he is hopeful that a strong data protection law would ensure security to the data that is being collected in various manners.

Data Protection Laws in India:

The Parliament had recently introduced the Data Protection Bill 2019, which has been referred to the Standing Committee on 11th Dec 2019 after being introduced in the Lok Sabha. The Bill is based on the recommendations of the 'Committee of Experts on Data Protection' headed by Justice B.N. Srikrishna. The Bill is soon to become the law governing Data Protection addressing privacy and security concerns. That does not mean sensitive, personal data was never protected in India. In fact, in a recent case involving a trio leaking sensitive information pertaining to account details of customers of a bank, a case was filed under the Indian Penal Code(IPC) and the Information Technology Act 2000(IT Act) upon a complaint by the bank itself..

The IT Act was an attempt to bridge the gap between law and advanced technology. The Act protects privacy in digital communication by providing cyber security. The IT Act provides cyber security to both devices as well as information stored in them from unauthorized activities. The provisions of the Act apply to any offence under the Act committed in or outside India, provided the computer system/network involved is located in India.

The Act was amended in the year 2008 inserting section 43A and 72A. These sections are relevant in relation to data protection in as much they impose liability on corporate entities to pay damages to persons in case of wrongful loss to the provider of information or wrongful gain to anyone else due to the negligence in maintaining and handling data with security, and also in imposing punishment for improper disclosures in breach of a lawful contract.

Now, it is also to be understood that at certain times the interception or leakages may not be always prevented. However, the standard that is required to be adhered to by the body corporates under section 43A is to provide reasonable security to the practices and procedures of data handling. But what is this reasonable security may be understood in the following ways:

1. Standard of security may be determined by the contract between the parties, or

2. Where there is no agreement, then following the requirements of the existing laws. For example, laws protecting 'Privileged Professional Communication' between an advocate and a client.
3. Any law/procedure prescribed by the Central Government. These Rules are now also referred to as section 43A Rules.

Moreover, these procedures are for collection and disclosure of only sensitive personal data/information and not for other information which may be available in public domain.

Despite the number of laws on privacy and the specific legislation of IT Act which includes digital privacy protection, a specific enactment for the protection of data privacy would bring the various strings together as a complete bundle or code. Specific Data Protection enactments lend teeth to the authorities to implement the security measures better and impose liability on specified parties/stakeholders and protect users from potential threats of privacy in a proper framework. Data Protection laws are more specific in identifying privacy intrusions and are capable of instilling trust in the public in relation to their private/confidential information. Most importantly, Data is now a commodity that may be bought and sold in the market. Thus, where on one hand data is compared to with oil refinery capable of earning millions for the corporates, it is also regarded as water by the think-tanks who insist on its free flow across the globe. Given the importance of a data-rich economy, a specific law regulating its transmission and protecting the interest of its source, i.e. the information provider, is more of a necessity than of feasibility.

Apart from that there are certain other Salient features of the Bill:

Specific terminologies of data principle, Data fiduciary and Data Processors by defining their roles clearly. Some data fiduciaries may be referred to as significant data fiduciaries due to various factors like volume and sensitivity of the data processed and probability of harm especially when a new technology may be adopted in data processing. It is a known fact that IOT is being used more than before as data collection tool. IOT's increasing marketspace for data collection as prediction tool, as production planning tool, as a strategy determination tool is going to play a crucial role in an information society. Thus, the role of data fiduciary to maintain integrity and transparency of the processes involved in collection of data, obtaining consent of data principal, ensuring use of data for only the pre-determined purpose and that the data so collected as a source of information is accurate and not misleading, etc. would put it in a trust-based relationship with other stakeholders involved. social media platforms or

websites, apart from mere business information providing platforms or mere search engines, come a significant stakeholder and carry higher responsibility in the maintenance of privacy. This is also pertinent considering the increasing use of IOT by online social media, especially for improving marketing strategies.

At the same time when government is itself experiencing a transition into e-governance, use of internet and connected smart devices for its purpose may impose few challenges. Real time tracking and analysing devices without proper safeguards may carry crucial information to hackers. Moreover, where a third party is involved for processing the data, the issues of national security become more pressing. The Aadhar case was impugned on one of the ground of data processing being done by private party. Only after being satisfied with the security measures taken in the process this issue was settled in favour of the State. Thus, every such processing of data must necessarily have to be tested on the anvil of proportionality of such measure vis-à-vis the risks it poses to security of nation. Thus, Government itself is also a stakeholder as data principal and fiduciary where its database security lapses can harm not merely few persons but the security of the whole nation.

One probable fix to security lapses could be the in-built measures in the design. The Bill does insist on the design policy and its constant review. The other most significant contribution of the Bill would be the additional responsibility imposed on data fiduciary as a guardian data fiduciary in case of a website or online services meant for children or who generally process a large amount of data pertaining to children and debars them from tracking or monitoring any kind of information of a child that may possibly harm the child's security or affect him in any manner. The significance emerges from the development of Smart Toys and other devices used for monitoring child activities.

Also, the Bill categorizes data into several categories. Anonymized personal data is outside the scope of protection under the Bill. The personal data processed must reveal the identity of the person. Thus, if an IOT device, capable of providing various information, which put together would provide valuable information about one's identity it could mean to reveal one's personal data. If the information is capable of revealing the identity of the person with respect to his financial data, biometrical data, caste, religious or political beliefs, or any such information identified by the government or the authority established under the Act, would be protected as sensitive personal information. Thus, if any company uses IOT based

devices capable of carrying such information, they need to be more vigilant to fence their data from leakage or theft or pilferage.

Data has also been classified as critical data but not defined. Whereas sensitive data can be transferred outside with the limitation of its storage being required to be done only in India, critical data may not be transmitted outside India. With the increasing use of technologies like AI or IOT, a lot of demand for Cloud market is going to increase but the way companies opt for cloud storage depending on various factors like cost and other storage options provided by the cloud computing service provider, it is likely to have effect on costs of companies. At the same time, there can be no assurance of enhanced security of data if it is to be stored within India.

Data Protection and Right to be Forgotten:

Right to be Forgotten is an essential aspect of privacy. This is even more relevant in the context of data being transmitted over devices and the marketing of such data. As has been shown that knowingly or unknowingly we tend to share different information which on the face of it may not seem to harm an individual but capable of projecting a valuable data for data collection firms and their use for business and marketing purposes. Thus, consent of not just the information shared but also its purported information is important and in the absence of such later consent, the individual must have a right to be forgotten. Of course, there are many issues pertaining to IPR, but that requires a separate analysis and study that is not the scope of this paper. The basic issue in this context remains that where such data collected belongs to certain category of persons, would they prefer to be forgotten once the purpose of such collection is over or continue to give consent for its use for some other purpose or use. For example, if a company collects data of different students searching for admissions into a law school, and then later sells the data to some University, the question would be whether the data principal may have a right to be forgotten as the data collected served its purpose of informing them about the admission process is complete and cannot extend to using this data to sell this to other colleges/universities for their benefit. This interpretation may be drawn to some extent on the basis of the new provisions in the PDP Bill.

RTI and Data Protection:

The objective of the RTI Act is to promote transparency whereas the existing data protection provisions and the Bill protect the privacy. The RTI stems from collective good

and social responsibility while data privacy respects individualism. These ideological differences lead to constant debate on which right is more supreme, i.e., Information or Privacy, or which aspect is more ideal, i.e., Collectivism or Individualism. This aspect may be dealt at this juncture without even venturing into the question whether data protection itself promotes collective or individual rights, for the time being. Where Right to Information is a basic right in democracy to know about the Government activities through the data possessed with it, Privacy is a fundamental and natural right that guards against unwarranted surveillance and pilferage of sensitive personal information into public domain.

Even though there is no specific Data Protection Act, section 72A imposes responsibility on an intermediary handling personal data from disclosing or causing to disclose it to a third person intentionally or knowingly that such disclosure might cause wrongful loss to such person whose data is disclosed without his/her consent. On the other hand, negligent handling of the data by a body corporate is also punished under section 43A. Thus, the IT Act provides protection to personal data of any person that is handled by other persons/ body corporates from any kind of intentional or negligent disclosures against the interest of the person concerned.

At the same time, it is equally allowed under the IT Act to disclose such information that may be already available in the public domain or which otherwise may be mandated to be disclosed by any law, such as the Right to Information Act, 2005.

The introduction of the Bill on data protection itself brought forth a new dimension to the standard of protection of personal data, whether electronic or manual. The 2018 Draft Bill proposed to limit the disclosure mandate under the RTI Act 2005 to cases which necessitate 'public activity or interest', which did not carry forward in the 2019 Bill.

In fact, the Right to be Forgotten after the fulfillment/completion of the purpose for which data was obtained from the data principle has itself been made subject to Right to Speech and Right to Information of another person while leaving scope to outweigh the latter.

Thus, the PDP Bill need not be perceived to be limiting the scope of the RTI. Rather, it adds a new right of an individual to seek information of his own data possessed by any Authority. Although this right is not specifically mentioned in the RTI Act, 2005, in few instances the courts have recognized it.The Data Protection Laws specifically provide this right. It is this right to information of one's own data with the Government and other authorities that is of

utmost importance in times when through technology every individual is under constant surveillance and every minute detail is available either through official electronic records or through social media. It is already explained earlier how the new technologies using IOT and AI transmit the data without actual knowledge of the person and the increasing use of such technologies by Government and its agencies.

Secondly, Data Protection Laws provide the right to seek personal information not merely against the Government Agencies but also against the private parties. Whereas under the RTI Act 2005 the information from the private sector may be sought only when they are substantially funded by the Government for the activity in relation to such information or at least where some element of control by the Government may be there.

Thus, given the larger role that right to information of one's own data, in the context of SMART Societies we are engulfed with, PDP Bill in the form of a specific data protection law will surely stand on higher pedestal than any other information pertaining to other individuals.

RTI and Data Protection are not conflicting rights but rather together further the objective of a more responsible sharing of information. The Bill in no way hinders transmission of information from relevant sources but imposes certain safeguards at the juncture of the Sources handling the data to address privacy compromises leading to more harm to an individual or society at large.

This brings us to the next dimension as to whether the existing laws and the 2019 bill offer an individualistic perspective of promoting privacy or rather deal with issues of common good of the society. Though the right of privacy is seen from the perspective of an individual's choice to be 'left alone' but the significance in holding privacy as a constitutional-fundamental right is way beyond such perspective. Right to privacy strives to achieve even collective good of the citizens and not merely an individual's right. Without privacy society cannot progress further, whether economically or socially. This is even more significant in a digital sphere where its benefits can be spilled over a large section of population only when it is not just easily accessible but is also a safe arena for the new players. Thus, digital economy and its' large outreach is least achievable if there no security for the data being shared and received.

Security of Data obtained by Government may be justified from the collective good concept but a blanket exception to government for interception of electronic data is inimical to this fundamental right guaranteed under the Constitution. In this context the observations made in the Aadhar case may be relevant where it was rightly pointed out by the apex court that where on one hand the people of the country have got right to information from the government, the unlimited access to private data of individuals and its possible use in arbitrary manner by the government, would undermine the free spirit of enquiry by an ordinary man with constant fear of himself being under scanner all the time. The Canadian Supreme Court's judgement holding he right to digital anonymity has laid down a higher standard for even the government to breach privacy and to have strong reasons to make interception even for investigative purposes.

The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009 provide safeguards against cyber security breaches, collection of traffic data, use of monitoring devices in viewing or inspecting traffic data and preventing its unauthorized access. Even the authorized agency cannot disclose the information or data for any purpose other than for use in detection or investigation of cyber threats or for traffic information. Almost after a decade after the notification of these Rules, the Government by its order dated 20th December 2018, notified the agencies authorized to lawful interceptions and the main concern that arose was whether any interception made before 2018 can be deemed to be with authority or not. It is pertinent to note that any information or data pertaining to such interceptions may not be disclosed by the Government in certain circumstances even where information is sought by anyone through an RTI application on the grounds that disclosure of such information would defeat the very purpose of the interception.

Of all what is discussed, the deplorable truth about Privacy in India is about lack of information about informational privacy. Ever since being raised before the court, there has been a momentum in understanding privacy. But Srikrishna Committee's Report and the Bill have accelerated the spread of awareness about the existence of a mechanism of data processing, about the privacy concerns of individual, about the importance of its protection and the ways and means of securing personal information.

Conclusion:

Data protection issues are most often restricted to the aspect of surveillance. Although, surveillance aspects are crucial to be considered in data protection, but from the standpoint of privacy it must go much beyond that. Surveillance is part of privacy issues. Privacy has a wide scope and is often vaguely defined, if at all. Even the GDPR of the European Union does not define what privacy is. However, given the data from various sources, it is quite impossible for a person to retain privacy in a world so well intertwined through connected things. Therefore, what is rather being sought to be protected is the use of such personal information for surveillance. Hence, the individual is satisfied if the information being retracted is not being intercepted by unlawful means by unauthorized persons for unjustified reasons. However, privacy rights claims can extend to the refusal of providing certain information, which though is possible to be leaked through smart devices even unknowingly. It also extends to right to know if any such information has been obtained, by what means and for what purposes. It establishes a ground for an individual to insist on deletion of such data i.e. right to be forgotten and to prevent its misuse. Data Protection Bill has rather accumulated all these privacy rights within its ambit. However, what remains to be seen when it becomes a law is how the various exceptions provided to certain purposes by data fiduciaries and more particularly to the Government, will exercised. Data fiduciaries, depending on the amount of and nature of data handled by them and the sensitivity in relation to the harm caused due to breach, have been subjected to various limitations to extract data and are required to provide utmost security to the data stored but whether the exemptions provided demonstrate the non-requirement of protection of data privacy from the government is yet to be seen. Even though Government Authorities had powers of interception and encryption of data even under the existing laws, the debates that arose on the Bill have definitely been able to garner more support for lesser intervention by the Government and the requirement of strong legitimate purposes for any compromise with the data. The new law has also indicated towards digital education right from a young age and need to be vigilant before exploring the benefits of new technologies. The IOT and other related technologies leave humans in such awe that it is difficult to resist from its usage. But it requires humans also to become smart to venture into this captivating SMART city, education, environment, security, etc. This also requires laws to be SMART because quite often laws are always believed to be behind technological innovations. But the Bill now would require data storage technologies to be more innovative and design the data transfer and storage in accordance with the requirements of the Bill.

Overall, it is too early to count the chicken and the benefits of the Bill but surely this is the right time for it to hatch into a full-fledged law amidst the ground that is already set for digital connection of devices and their communication.

ROLE OF LAW IN E-COMMERCE ACTIVITIES

M. Athma Rubavathi[417], S Prasanna[418]

ABSTRACT

This paper is discussed about the interface between the E-commerce Laws and E-Commerce. This is also known as electronic commerce and internet commerce. In this E-commerce activities peoples are transacting the goods and services, transfer the funds and exchange the data. So, services are provided over the internet. In this developing global technical society most of the peoples are like the e-commerce activities because of the reasons of faster buying process, any time we can buying/selling, easily select product from different providers without moving around physically, Time management for his/her own purpose or business purpose. E-commerce offered many advantages to companies as well as customers but it also caused many problems. There are many bad sites lose customers money, no guarantee of product quality, lack of awareness of the customers. Other than this issues some legal issues like minors' contracts are also there in the e-commerce activities. Security of the customer information's providing during the online transaction is another issue in the E-Commerce activity. Crypto Currency is the one of most riddle thing in E-Commerce network. Crypto Currency is virtual form of dejure currency. Legality and Centralisation is the first and most important issue in Crypto Currency. So, in this paper we are discuss about the issues in the E-Commerce Activities and how the law protect the consumers.

1. INTRODUCTION

E-Commerce is a trending word in world wide. Buying, selling, transferring or exchanging good, service, data or information over the internet communication is called E-Commerce Activity. E-Commerce are running with various type like business-to-business (B2B), Business-to-Customer (B2C), Customer-to-Customer (C2C), Etc., E-Commence evaluates itself time to time suitable with society. In India, E-Commerce starts its turn and it has rapid growth in India. In India like Amazon, Flipcart, OLX, OLA, UBER, Zometo are grate examples to E-Commerce Companies. In fact this industry made great changes in Indian technology society. It comes through every one's smartphone. In world-wide also it become super series. Because it saves more money and time of consumers and vendors. It expanded small village to metro polluted cities. Even there is a benefit there is huge issues and problems. And in this paper we are analyse and discuss about the following sections.

[417] Assistant Professor, School of Law, SRM Institute of Science and Technology, Kanchipuram, Tamil Nadu. athmarm@srmist.edu.in

[418] S. PRASANNA, Student pursuing B.A., LLB, Government Law College, Trichy, Tamil Nadu. prasannasri26092001@gmail.com

2. OBJECTIVE OF STUDY

The study aims at the following objects:

- To study the current scenario of E-Commerce Activity in India.
- To analyse the major issues in E-Commerce Activity.
- To analyse the how the law get the role in E-Commerce Activity and how the law protect consumers.

3. LITERATURE REVIEW

'***A Study on Future and Challenges of Electronic E-Commerce in India***[419]' (2020) in this paper **Mrs. Neha Narang** examines the challenges and future of E-Commerce. And she defined E-Commerce is "electronic commerce which means activities of exchange of products, and information with the help of internet." And this paper deals with 2019-2020 scenario of e-commerce in India, future of E-Commerce in India, Forecasting Using Liners Regression and the barriers of e commerce. She suggests that Government should take steps to provide a proper legal framework so that hurdles in the growth of e-commerce are reduced to minimum. But, she didn't focus on the law and the E-Commerce are play them role in society. According to the chief editor of International Journal of Electronic Commerce, **Vladimir Zwass**, "E- commerce is the exchange business data, keeping business dealings and organizing business activities by means of Mobile networks". Further Zwass said that E-Commerce has been redefined by the dynamics of the Internet and typical e-commerce is rapidly shifted to the Internet. According to **Sarbapriya Ray**'s, '***Emerging Trend of E-Commerce in India: Some Crucial Issues, Prospects and Challenges***[420]' (2011) E-commerce is a gold mine if it run without adequate legal protection, it will become a landmine to society. **Ashok Panigrahi**, **Ranjan Upadhyaya** and **Dr. P. P. Raichurkar** researched on their paper of '***E-Commerce Services in India: Prospects and Problem***[421]***s***' (2006). They defines E-Commerce is a new way of organizing, managing and executing business activities using of computer and telecommunication networks. They only discuss about socio and political factors, they did not consider law's important and how taxation and contract place main role in E-Commerce Activities. **Ritu Sharma** and **Himanshi Babbar** in their paper of '***Future Aspects and Challenges of E-Commerce***[422]' (2016), they explain Electronic Commerce refers to the huge range of online business activities for the goods and services. It also pertains to any form of business activities in which many people and parties are interact with

[419] Mrs. Neha Narang, *A Study on Future and Challenges of Electronic E-Commerce in India* (6th edn. International Journal of Multidisciplinary Research 2020) 58.
[420] Sarbapriya Ray, *Emerging Trend of E-Commerce in India: Some Crucial Issues, Prospects and Challenges* (2nd edn. Computer Engineering and Intelligent System 2011) 17.
[421] Ashok Panigrahi, Ranjan Upadhyaya and Dr. P. P. Raichurkar, *E-Commerce Services in India: Prospects and Problems*, (3rd edn. International Journal on Textile Engineering and Processes 2016) 9.
[422] Ritu Sharma and Himanshi Babbar, *Future Aspects and Challenges of E-Commerce* (7th edn. Biz and Bytes 2016) 131.

electronically instead of any direct physical contact. In ***'Growth of E-Commerce in India[423]'*** (2015), **Dr Kishore Kumar Das** and **Affreen Ara** gave their definition about e-commerce is , "E-Commerce is including the activities of buying and selling and exchange of goods and services or transmitting of funds or data, over an electronic system, primarily the internet". And they researched on E-commerce growth, market potential, key challenges, and future of E-commerce in India. **Aijaj Ahmed Raj** and **Wazida Rahman** are researched on their paper of ***'E-commerce Laws and Regulations in India: Issues and Challenges[424]'*** (2016), and the observed that the rapid growth of E-Commerce has shown the need for vibrant and effective regulatory mechanisms, which would strengthen the legal infrastructure that is crucial to the success of e-commerce in India. They describe the present laws and regulations governing e-commerce and examine the challenges and opportunities of e-commerce under the present legal regime in India. They are missed to discuss about the how the law protect customers and how the customer affected by major issues of E-Commerce. **Grisha Agarwal** researched on the topic "***E-commerce: Opportunities and Challenges in Online Business[425]***" (2016). This paper examines different opportunities of e-commerce. This paper shows the various challenges and opportunities of Indian E-commerce. **Partha Pratim Dey** made a study on bitcoin with the title of ***'Cryptocurrency: Its Implications and Legal Status in India[426]'*** (2019). He study the implications and the current regulatory framework for cryptocurrencies in India. And he fully discussed bitcoin's evaluation and how it's going and what are the types of earnings of bitcoin. And also he describe the barriers and benefits of bit coin. **Tamradaman & Nagpure** (2017) in the paper '***Bitcoin in India[427]'*** identified the various legislations which will regulate the Bitcoin in India if it is recognized as a legal tender in India. The author concluded that to be considered a global currency the wide fluctuations in the value must stabilize. **Pandey** (2018) in his paper of ***'"Bitcoin" As Emerging Virtual Currency and Its Related Impact on India[428]'*** analysed the return of Bitcoin for the period 2013-17 and concluded that it is earning a handsome return but has high volatility. After demonetization Bitcoin has become more popular in India. The author also warned the investors about the grave danger associated with such currencies in his paper. ***'Bitcoins in India: A Study of Legal and Economic***

[423] Dr Kishore Kumar Das and Affreen Ara, *Growth of E-Commerce in India* (2nd edn. International journal of Core Engineering & management 2015) 25.
[424] Aijaj Ahmed Raj and Wazida Rahman, *E-commerce Laws and Regulations in India: Issues and Challenges* research gate 2016, <https:www.researchgate.net/publication/330845555_E-commerce_Laws_and_Regulations_in_India_Issues_and_Challenges> accessed 10 February 2021.
[425] Grisha Agarwal, *E-Commerce: Opportunities and Challenges in Online Business* (11th Biyani International Conference 2016) 405.
[426] Partha Pratim Dey, *Cryptocurrency: Its Implications and Legal Status in India* (2nd edn. Handbook on management Practices (collection of Chapters) 2019) 142.
[427] Tamradaman, A. and Nagpure, S. *Bitcoin in India* (8th edn. International Journal of Computer Science and Information Technologies 2017) 421.
[428] Pandey, P. K. *"Bitcoin" As Emerging Virtual Currency and Its Related Impact on India*, (2nd edn. International Journal of Latest Engineering and Management Research 2017) 59.

Aspects[429]***'*** (2018) In this paper **Kumar M** made a research on bitcoin and he states, "if remain unregulated will, poses a threat to financial stability. However, the technology behind it can be used by banking industries for making secure transactions". In this paper he focus only bitcoin's characteristics. He didn't go with other crypto currencies and how the law get role on that. **Atif Aziz** discuss about his ***'Cryptocurrency: Evolution & Legal Dimension***[430]***'*** (2019) a brief history of the evolution of currency and the environment in which the first cryptocurrency and Essential features of currency and its presence or absence in cryptocurrency are discussed in his paper. He explain Cryptocurrency is a natural evolution of currency in the internet era. It is fast, efficient and a secure medium of exchange with huge cost saving benefits.

4. ISSUES IN E-COMMERCE ACTIVITES

Here we analyse major issues of E-Commerce Activities. Issues ae Followed By:

- **Legal Validity of E-Contract**

Indian Contract act states when there are no capacity[431] and no consideration[432] and then there are no contract. But In E-Contract like click-warp, shrink-warp, and browse warp are conducting for a formality. But there is no consideration by the consumers. Here maximum of E-Consumers doesn't read the terms and conditions of every apps and websites. And the websites and apps are allows their services to below the eighteen age peoples. And also restrict the minors[433] to involve in the E-Contract. Here a question arises that how this type of E-Contracts are have Legal Validity.

- **Out Dated ITA and Data Theft**

The Information Technology Act, (*herein after ITA*) 2000[434] enacted with the preamble of, 'provide legal recognition for transition carried out by means of electronic data interchange and other means of electronic communications'. Now here are many more various development in technology industry. But, ITA is doesn't amend for the current technological issues. This paper also discuss about this issue.

- **'Just Like' E-Consumers**

E-Consumers means who are consume a product or service over the internet. They are don't concentrate what they are doing. Consumers are take it easy that how and what the

[429] Dr. Mohan Kumar, *Bitcoins in India: A Study of Legal and Economic Aspects* (20th edn. Journal of Business and Management 2018) 75.
[430]Atif Aziz, *Cryptocurrency: Evolution & Legal Dimension* (18th edn. International Journal of Business, Economics and Law 2019) 31.
[431] The Indian Contract Act 1872, s. 2(d).
[432] The Indian Contract Act 1872, s. 11.
[433] The Indian Majority Act 1875, s. 3(1).
[434] The Information Technology Act 2000.

intellectual business companies are using their personal data and how its effect was. It's so benefits for that intellectual business companies.

- **Challenges in Centralization**

E-Commerce activates are working within any part of the world. And here crypto currencies (*herein after CC)* are given new dimension of currency's history. In India CC are still have confusion status. Because, Executive and judicial bodies are they take their decision in contradictory. But the consumers are suffered by these confusing decisions. This paper mainly discuss about above the issues.

5. METHODS AND RESULTS

This paper broadly used an expletory research technic based on past literature from respective journals and report from government authorities extensive academic literature on E-Commerce activates. According to the objective of study, the research design is of descriptive nature. We take Primary data from consumers by retrospective survey method. That survey taken by Google Forms Platform. In this survey totally hundred consumers were polled their answer. And Available secondary data was extensively used for the study. The present study has been undertaken to comprehend how the law place its role in E-Commerce Activates and how it protect consumers in India.

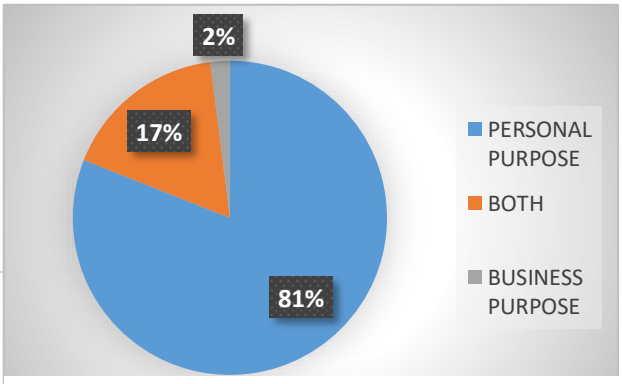
Following sections summarise the findings from the field survey for the E-Commerce Activities. For this survey, a Single page questionnaire was developed in the Google Forms (annexure 1). Most of the questions were framed as multiple Choose or with a defined set of possible answers. The questionnaire comprised 24 closed and open questions, divide into different themes are like E-contract, E-Shopping and Activates. From this survey are summarized in Tables 1-5 and Figure 1-14

Figure 1 ***Reason of E-shopping***

**Source Author's estimation from field survey data*

Figure 1 shows the tread in E-Shopping and E-Commerce Activates in India. The Consumers Prefer E-Shopping for Best Deals (44%) more than Time Conception (41%). This figure also shows E-Consumers Didn't trust online products safety (7%) less then online product quality (8%).

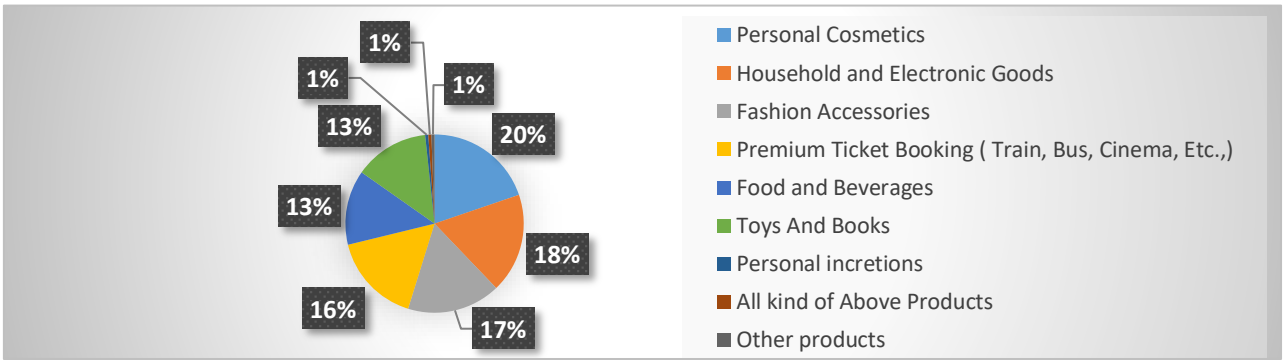
Figure 2 Purpose of E-Commerce Activates



**Source Author's estimation from field survey data*

Figure 2 shows Consumers buying and selling purpose in E-Commerce Activities. 81% consumers are only use E-Commerce for personal purpose. 2% consumers use E-Commerce for business purpose. 17% of Consumers use E-Commerce for both purpose.

Figure 3 ***Type of Good are Purchase from E-Commerce Websites***



**Source Author's estimation from field survey data*

Figure 3 is expose which type of products are purchased by consumers. We dived 7 type of goods of online purchasing goods. Firstly personal cosmetics (20%) is the consumers most purchased goods from E-Commerce Websites. House hold and Electronic Goods (18%), Fashion Accessories (17%), Premium Ticket Booking (Train, Bus, Cinema, Etc.,) (16%), get their place in next to next. Food and beverages (13%) and Toys and Books (13%) are equally purchased from E-Commerce Websites. And finally Personal incretions (1%) and other Products (1%) get last place of figure.

Table 1 ***Distribution of consumer's Buying Product by Buying Purpose***

OPTIONS RESULTS

Buying Product\Purpose	**Personal**	**Business**	**Both**
Personal Cosmetics	94.3	2.9	5.7
Household and Electronic Goods	84.4	0	15.6
Fashion Accessories	93.3	0	6.7
Premium Ticket Booking (Train, Bus, Cinema, Etc.,)	86.2	0	13.8
Food and Beverages	87.5	4.1	8.3
Toys And Books	87.5	0	12.5
Personal incretions	100	0	0
All kind of Above Products	100	0	0
Overall	91.7	0.9	7.8

**Source Author's estimation from field survey data*

Table 1 presents the distribution of consumer's buying Product with respect by buying purpose. Some 94.3% consumers of personal cosmetics are buy this for personal purpose. And 5.7% consumers are buy it for both personal and business purpose. Others are buy it for business purpose. This table shows Personal Incretions (100%) are bought only for personal purpose from the E-Commerce

Websites. And from Business purpose, Food and Beverages (4.1%) category is most bought category from it. Most of the category didn't buy for business purpose. Household and electronic goods are bought for both personal and business purpose. In overall Personal purpose (91.7%) goods are take much pore place in E-Commerce activates.

Table 2 ***Distribution of consumer's Buying Product by Reason of Ecommerce Shopping***

OPTIONS	RESULTS				
Buying Product	Best Deals	Best Quality	Time management	Safety	Others
Personal Cosmetics	45.7	2.9	37.1	5.7	8.6
Household and Electronic Goods	34.3	18.8	34.4	0	12.5
Fashion Accessories	50	6.7	30	3.3	10
Premium Ticket Booking (Train, Bus, Cinema, Etc.,)	27.6	10.3	48.3	3.4	10.3
Food and Beverages	45.8	0	45.8	0	8.3
Toys And Books	25	4.1	50	8.3	12.5
Overall	38	7	41	3.5	10.5

**Source Author's estimation from field survey data*

Table 3 presents distribution of buying Product by Reason of E-Commerce shopping. Best deals wise food and beverage (45.8%) category is get more place in E-Commerce Website Industry. Best Quality Wise Household and Electronic Goods (18.8%) category is get more place in E-Commerce Website Industry. Time Management Wise toys and books (50%) are more comfortable for Consumers in India. In safety Wise consumers trust toys and books (8.3%) are more than others. And also personal cosmetics are bought for best deals (45.7%) then time management (37.1%). Premium Ticket Bookings are bought for time management (48.3%) then best deals (27.6%).

Figure ***4 Consumer's Involvement in E-Commerce Activates***

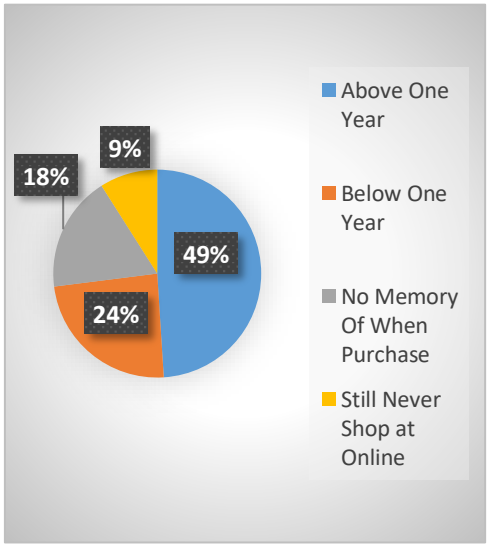


Figure 4 presents new trend of E-Commerce in India. 24% Consumers are started involvement In E-Commerce below one year. And 49% of consumers are using E-Commerce above one year. 18% consumers don't have memory of when they start purchase in E-Commerce Websites. And still 9% of Consumers never shop at online.

Table 4 Presents Distribution of Consumer's online involvement by gender and employment status.

**Source Author's estimation from field survey data*

Table 4 ***Distribution of People's online experience by gender and Employment status***

OPTIONS RESULT

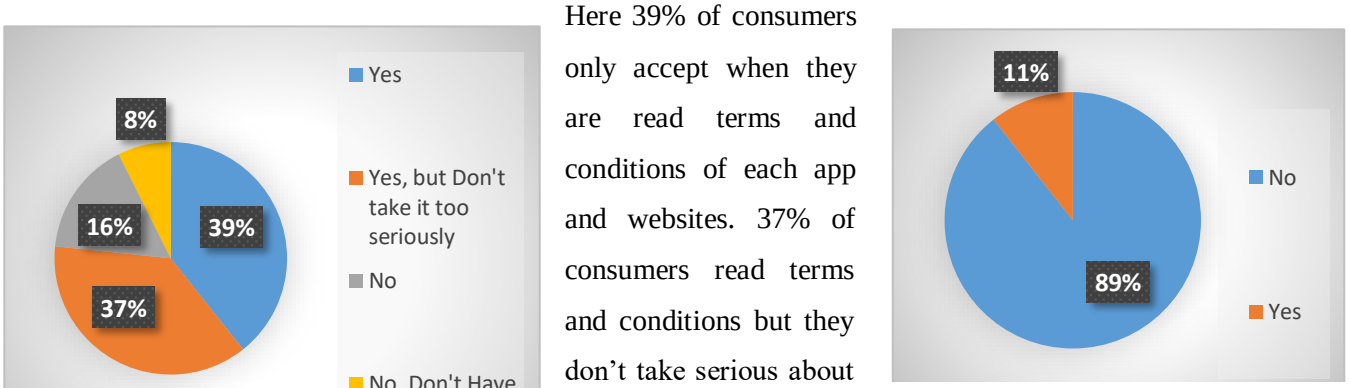
DURIATION	MALE	FEMALE	Student	Private Emp.	Unemployed	Others
Above One Year	44.9	55.1	69.4	20.4	6.1	4
Below One Year	41.7	58.3	91.7	8.3	0	0
No Memory Of When Purchase	27.8	72.2	77.8	0	22.2	0
Overall	38.1	61.9	79.6	9.6	9.4	1.3

*Source Author's estimation from field survey data

In gender wise women (61.9%) are more involved in E-Commerce all the period of this industry. In table 4 clearly shows that students (91.7%) are the most category of involvement in E-Commerce within one year.

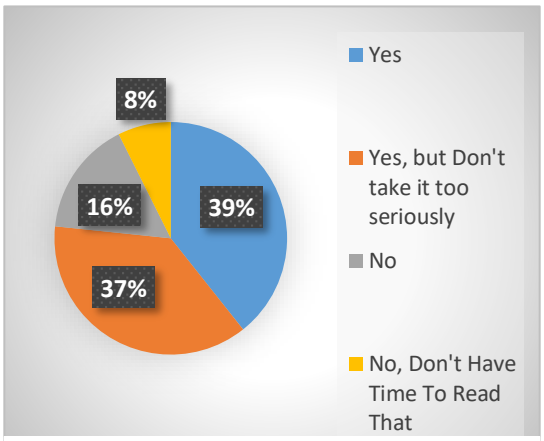
Figure 6 ***E-Contract Involvement***

In our survey 89% of Consumers polled the never involved in E-Contract. And 11% of consumers polled that they are involved in E-Contract.



*Source Author's estimation from field survey data

Figure 7 ***How the Consumer read Terms and Conditions***



*Source Author's estimation from field survey

Here 39% of consumers only accept when they are read terms and conditions of each app and websites. 37% of consumers read terms and conditions but they don't take serious about it. 16% consumers didn't read terms and conditions. 8% of consumers don't have time to read that.

Table 5 ***Distribution of Consumer's Answer of How the Consumer read Terms and Conditions by who involved in E-Contract***

OPTIONS RESULT

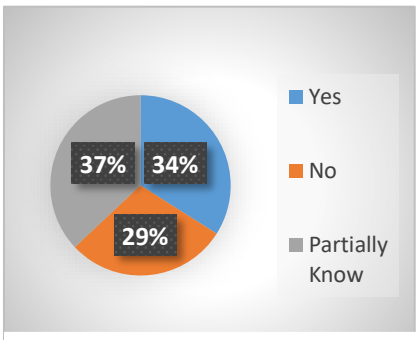
	Involved in E-contract	Never Involved in E-contract

Yes	18.1	81.1
Yes, but Don't take it too seriously	2.9	97.1
No	6.7	93.3
No, Don't Have Time To Read That	14.3	85.71

**Source Author's estimation from field survey data*

Table 5 presents Distribution of Consumer's Answer of How the Consumer read Terms and Conditions by who involved in E-Contract. In fact 81.1 of who read the terms and conditions of each app and website, they don't have knowledge of that is an E-Contract.97.1% who don't take serious about terms and conditions, also they don't have knowledge of that is an E-Contract.

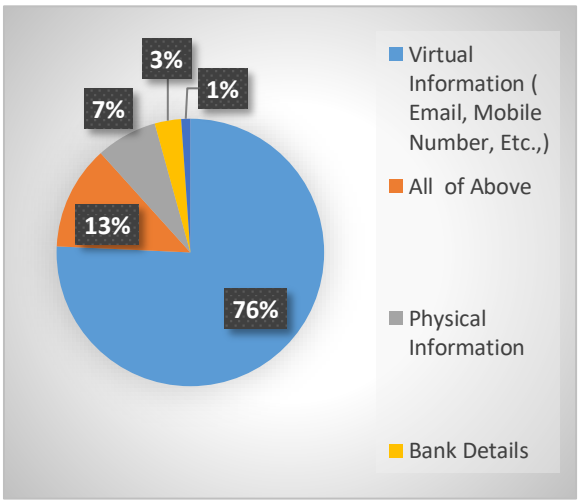
Figure *8 Question to Consumer that Are you Know you are sharing your personal data to E-Commerce Websites*



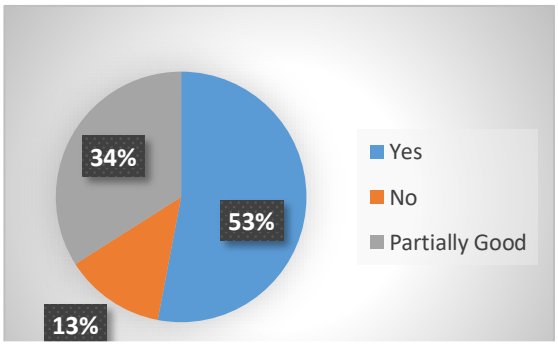
**Source Author's estimation from field survey data*

Figure 8 presents Question to Consumer that Are you Know you are sharing your personal data to E-Commerce Websites. From our survey 29% Consumers Don't Know they are sharing them personal information to E-Commerce Websites. 37% of consumers partially know they are sharing them personal information to E-Commerce Websites. 34% of consumers know they are sharing them personal information to E-Commerce Websites.

Figure 9 *Types of information shared from Consumers to E-Commerce Websites* Figure 9 presents Types of information shared from Consumers to E-Commerce Websites. 76% E-Consumers shares their Virtual Information like Email, Mobile Number, Etc., 11% of consumers shares their all information includes virtual information, physical information, and bank details. 7% consumers shares their physical information. 3% consumers shares their bank details to the E-Commerce Web sites.



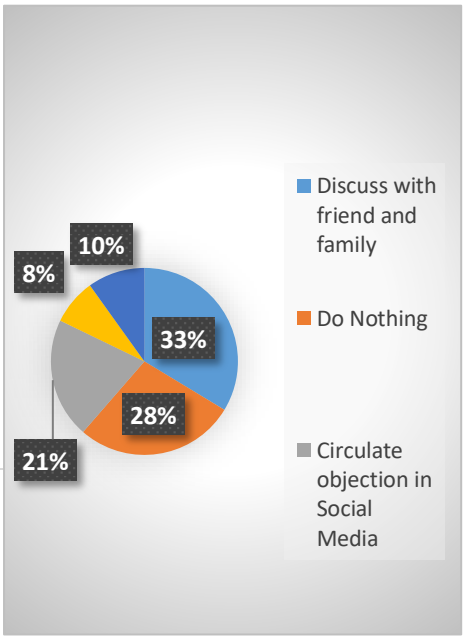
**Source Author's estimation from field survey data*



**Source Author's estimation from field survey data*

Figure 10 *Quality goods and Services from E-Commerce Activates*.

Figure 10 presents Quality goods and Services from E-Commerce Activates. 53% E-Consumers receive

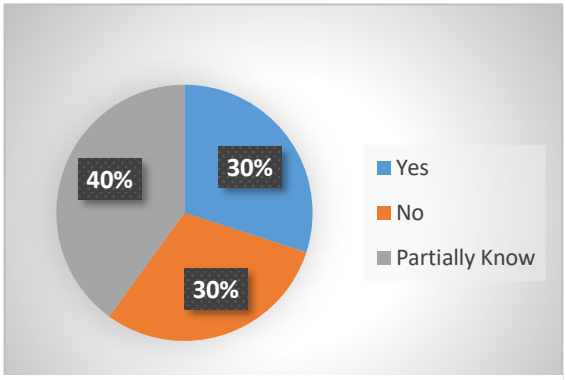


quality goods and services in E-Commerce Activates. 34% E-Consumers receive partially good products from E-Commerce Activates. 13% .Consumers not get quality products from E-Commerce Activities.

Figure 11 ***Consumer's action take on misleading advertising***[435]

Figure 11 presents how the consumer take actions on misleading advertising. 34% of people only discuss about the advertisement with friend and family circle. And seriously 28% consumer and people were don't take any action of that misleading advertisement. 21% of people were circulate objection of that advertisement in social media. 8% of consumers report that to media. **Figure** ***12 Aware of E-Commerce Related Laws***

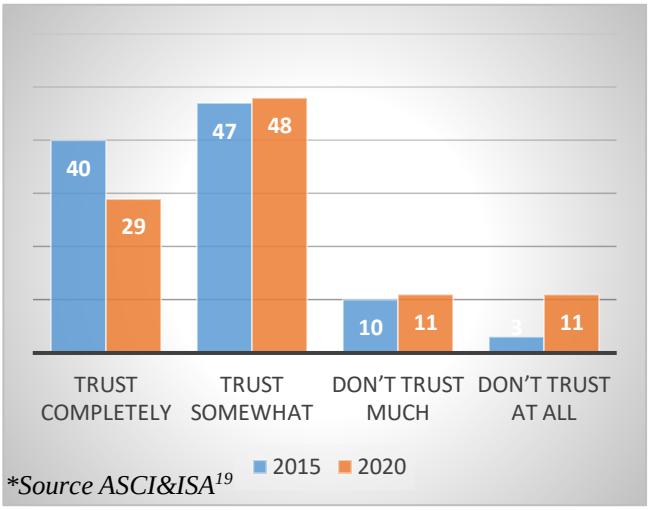
Figure 12 presents Aware of E-Commerce Related Laws to the E-consumers. 30% of consumers Aware of E-Commerce related laws. 30% of Consumers don't have awareness about the E-Commerce related laws. 40% consumers partially know about E-Commerce related laws.



**Source Author's estimation from field survey data*

Figure 13 ***Trust of Advertisement in websites in India.***

Figure 13 clearly shows that E-Consumer's trust on websites are down in the period of 2015 to 2020. It increase 3% to 11%, who don't trust the website advertising.



**Source ASCI&ISA*[19]

6. DISCUSSION

Now we take many results from the above results. This part take this paper to find the issues are how it still live in the E-Commerce Activities of India. First of all this section discuss the E-Contract of Website and apps (*herein after WAA)* to consumers. Every WAA are have their term and conditions. And all of the mobile phones and internet users are accept any one of the terms and conditions in our life. Figure 6 & 7 are explains how E-Contract are conducting. Because 93.3% of consumers are don't know that term and conditions are an E-Contract. Sole mind, negotiation, consideration and capacities are the basic elements of contract. But In E-Contract like WAA they didn't consider this elements they place a accept option for a formality. WAA uses this E-Consumer's ignorance. Secondly, insufficient effectiveness of ITA was big issue in E-Commerce in India. ITA Section 10A deals with E-Contract and WAA is Completely Alien.

[435] Advertising Standards Council of India (ASCI) & Indian Society Advertisers (ISA)'s survey of 'Trust in Advertising' (September, 2020).

Penalties and imprisonment are not satisfied with the damages of consumers. And one more think all this legal data theft are organising for Targeted Ads. Targeting ads are now trending and grow thing industry. Many Malty National Companies are investing in this field for their products. Nowadays Website Advertisements are losing its trust because of misleading advertising. It's proven by survey taken by ASCI&ISA[436]. Today we know how the targeted ads industry development by WhatsApp Privacy Policy Update[437]. Not even only the companies are the liability of this issues. 'Just like' Consumers means who don't care about his conception. This type of consumers in our society increase in recent years. Figure 13 shows how the people handle the misleading advertising. And also figure 14 shows how many consumers aware of the E-Commerce related Laws. This is why companies are being carried out by such actions of E-Consumers. Because, this make lead to terrorism, black money cornering, black money to white conversion etc., in recently Mr. Narendra Modi's Tweeter Account was hacked by John Wick and demand for bitcoin[438]. But Indian Executive and Judiciary bodies are release their contradictory decision. RBI bans Virtual Currency for misleading usages[439]. But in Internet and Mobile Association of India Vs RBI[440] the Supreme Court ruled that RBI don't have the jurisdiction on Crypto currency. Here for crypto currencies running free with decentralization.

7. SUGGESTION & CONCLUSION

We are live in fast forwarding world. We can't stand and watch that what are happening here. But we can run with a secure society. Secure means by us and for us. E-Commerce is the best innovation of this society. But, No matter what the government does, it will continue to change the mind-set of the people. From above Survey and literature research we are given some suggestion to Indian Government and Finance Ministry of India and The E-Consumers:

- Special Provisions for E-Contract in the Contract Act.
- Separate Department for E-Commerce Industry.
- Enact The Personal Data Protection Bill, 2019.[441]
- Separate Guidelines or Act for Virtual Currencies.
- Whatever government rule are enact, The Consumers should read each and every term and conditions of every Websites and Apps and make it subject to his knowledge.

[436] Figure 14.
[437] WhatsApp Privacy Policy Update, 2021, *available at:* https://www.whatsapp.com/legal/privacy-policy (last visited on January 24, 2021).
[438] Yuthika Bhargava, "PM Modi's Twitter account hacked" (The Hindu, 03 September 2020), <https://www.thehindu.com/news/national/twitter-confirms-account-of-pm-modis-personal-website-hacked/article32510247.ece> accessed 10 February 2021.
[439] RBI/2017-2018/154 DBR.No.BP.BC.104 /08.13.102/2017-18
[440] Writ petition (Civil) No. 528 of 2018.
[441] Bill No. 373 of 2019

E-COMMERCE CHALLENGES AND THEIR SOLUTIONS UNDER CONSUMER PROTECTION ACT, 2019 AND CONSUMER PROTECTION (E-COMMERCE) RULES, 2020

Supriya Madan Patil,[1] Deepti Madan Patil[2]

Abstract-

We are living in the Techno-savvy world and Technology has become part of our life-style. One of the influencing technology based sector is E-Commerce or Electronic Commerce. E-Commerce is buying and selling of goods or services through electronic networks mainly via internet. It also includes transmitting funds and data through electronic networks which are required for such transactions. E-Commerce is an emerging trend now a day and preferred by many traders as well as consumers over the traditional ways of trading. It is convenient, provides wide range of varieties and choices and these transactions can be done at any time from any place. However it also has its own issues and challenges like poor infrastructure, unavailability of tools, privacy and security issues, price manipulation, and misleading advertisement and so on. The Central Government has enacted Consumer Protection act, 2019 and Consumer Protection (E-commerce) Rules, 2020 to tackle these problems. We have discussed the benefits and drawbacks of E-Commerce and the challenges faced by consumers during e-transactions. We have also analyzed the safeguards provided under the Consumer Protection Act, 2019 and Consumer Protection (E-Commerce) Rules 2020. These provisions have provided better safeguard and protection to the consumers. Nevertheless, there is scope of improvement to meet some emerging challenges.

I. Introduction

One of the revolutionary developments the world has witnessed in last century is the internet evolution. The internet is network of networks which has made the world come together at the click of a computer mouse. It not only has facilitated worldwide communications but also revolutionized trade and commerce through electronic media. The evolution of internet has witnessed the growth from sending an email to purchasing and selling almost any product and services under the Sun from books, food articles to smart phones, airline tickets, banking, and online payment and so on.

Electronic commerce or E commerce is a revolutionary model of commerce. E commerce is buying and selling of goods or services using electronic media or internet and it also include the transfer of money and data for the execution of these transactions. Since its inception E- commerce

[1] Supriya Madan Patil, Assistant Professor, Bharati Vidyapeeth's New Law College, Kolhapur
E-mail- asst.prof.supriyapatil@gmail.com
[2]Deepti Madan Patil, Assistant Professor, Bharati Vidyapeeth's New Law College, Kolhapur
E-mail- asst.prof.deeptipatil@gmail.com

has grown rapidly. Now it has become the essential part of our lifestyles. Now the consumers need not go from shop to shop looking for products or services. E commerce has brought the shops at the door of consumers on their computer screens where they can shop from wide range of products and services at different prices and can enjoy different choices. Consumers do not need to carry cash or shopping bags; the goods and services can be paid by online payment and are delivered at their doorsteps. There are many advantages of E commerce but it also has its own drawbacks and challenges such as poor infrastructure, unavailability of tools, privacy and security issues, misleading advertisements, price manipulations, defects in products and services return and refund issues etc.

To tackle these problems and to provide better consumer protection the Central government has introduced the Consumer Protection Act, 2019 on 20th July 2020 and notified the Consumer Protection E commerce Rules 2020 on 23rd July 2020. These include various duties and liabilities of e commerce entities which brought fairness, security and clarity. However there are some ambiguity and lack of proper guidance regarding certain aspects which need to be addressed.

II. What is E Commerce?

E commerce i.e. Electronic Commerce is used by the companies, individuals for buying and selling of products and services via electronic media or internet or transmitting the data, money or funds through electronic media or internet and covers electronic transactions such as payments gateways, internet banking, online auctions etc.

The Consumer Protection Act 2019, defines E commerce as - "e-commerce" means buying or selling of goods or services including digital products over digital or electronic network"[3]

E commerce has been proved to be an effective alternative to brick and mortar store system, and now a days buying and selling goods and services online through online platforms like Amazon, E-bay, Etsy has become part of routine life. E commerce includes online transactions by businesses, consumers, vendors and other suppliers.

There are different models of E commerce which are enlisted as follows-

A. Business to Business (B2B)-

It is the e commerce between business to business where there is exchange of products or services or data information between business entities like manufacturers, retailers, traders via electronic media. For examples manufacturers may order the raw products that are needed when they require it.

[3] Consumer Protection Act, 2019,s.2(16)

B. Business to Consumers (B2C)-

It is most popularly known model and covers the online shopping, buying or selling of goods and services through internet. Amazon, Flipkart and such other platforms provide a facility to multitudes of traders, sellers and buyers to come together and transact. Some sellers own their own product or service website where customers can browse through range of products and buy them. Internet banking, online payments also come within the purview of this model.

C. Consumers to Consumers (C2C)-

Here, the transactions are between consumers, where consumers trade the products services or information with each other. Online auctions are best example of such model.

D. Consumers to Business (C2B)-

It deals with the electronic transactions where consumers make their products or services available to business companies for purchase. The companies bid and purchase the products or services or information. Examples include where a Software engineer make available his software for purchase to company or where a photographer stocks his photos to be purchased online by businessmen.

E. Business to Administration (B2A)-

This model includes the online transactions between business and government bodies or public administrations. E services are provided to government bodies through this model. Example is tax payment to government through third-party

F. Consumer to Administration (C2A)-

It is electronic transaction between consumers and the government bodies. Example is online lectures, health service payments etc.

Since its inception the E commerce has rapidly grown and has seen the online shopping from simple books, foods and other goods and services to online banking, ticket booking, payment gateways, and security to the online payments with advancement of technology.

III. Advantages of E-Commerce-

E-Commerce is a convenient, easy to access, time saving platform which provides variety of choices to the consumers. There are many advantages of E-commerce because of which it is most preferred by consumers now a day.

Global Market-

E-Commerce provides huge market where a person can buy or sale products and hire services all over the globe. It also creates competitiveness which is healthy sign of business economy. Varieties of products are available online and consumer can have better options and price comparison for the products or services. One can browse any product and purchase it which may not be available

in the local physical markets. For a trader larger number of customer is available to purchase products. There is no geographical limitation and the whole world can be your market place.

Time saving-

On the click of the button what you want to shop can be available. E-commerce is very much time saving and in very less time consumers can checkout various products and buy it. No need to travel to buy any product or hire any services. No need to wait in queues like in that of brick and mortal store in case of rush.

Cost effective-

Many options are available therefore one can buy product as per budget and requirements. Products are delivered to the doorstep of the customer. He needs not to bear travel cost. Many products are available on discounted prices also. Traders don't require building a physical store and maintaining it, which is beneficial to them especially for small traders and businesses.

Provide Choices-

If at physical store you can check out hundred different options, E-commerce provides thousands of different options of the product you are looking for. You can compare the prices, product quality through reviews etc. Some products are also tagged as best seller and you can come to know that the product is more preferred and bought by the other customers. E-commerce provides comparison shopping for the consumers.

Convenient-

E-Commerce websites are available 24*7 and 365 days of the year. It is thus very much convenient not only to the customers but also to the merchants. It is open all the time thus a person can shop at any time and from any place. For a trader, such availability increases the number of orders which is profitable for him.

Profitable market-

For a trader the advertisement and marketing cost is low. Creative marketing techniques such as videos of products can be used to attract the customers. A trader also needs not to spend money on building large infrastructure and maintaining it. There are no issues of stock control etc. Digitalization reduces the paper work. As the customers can place orders at any time from any place, merchants get large number of orders. With minimum capital the traders gets national as well as international markets for their businesses. It is easy to start and manage business online. Expand business or downsizing it is also easy.

Product information and reviews-

Information about a product or services is readily available on the website and can be read at a glance. Unlike the physical stores, on e-commerce websites customers can see the reviews of other customers about the products which help the customer to get better idea about real quality of that product.

Availability of goods and services-

Many products are not available to the local shop stores but can be bought through online shopping. People from remote places also can buy products which are not available at their local place.

Customer information-

E- Commerce websites collects the customer's data like name, e-mail, contact number, what sites we visited, and our interests and so on. Such kind of information is used to build a strong communication and retarget the customers to buy products.

IV. Disadvantages of E-Commerce-

Though E-Commerce is very convenient and has so many benefits, it has some disadvantages also. Data privacy and security issue, misleading advertisements, defects in goods and services and poor infrastructures are of major concerns.

Poor Infrastructure-

Internet connection is required to visit websites and even high speed network is required for e-commerce sites to run smoothly. Slow networking creates difficulties in online shopping. Smart phones are required for such online trades. Especially rural consumers and person who lives at remote places cannot purchase products online because of such poor infrastructures.

E-commerce websites gets crash some times and no one can buy products at that time. Website crashing is an unpleasant experience for a customer and they might avoid such sites in future.

No trial-

Customer can't get trial of online products before purchasing it. There is no personal touch and feel of the product buying online so as to assure quality. Some sites provide chat option with staff to get more information of product but it is not common practice and won't be compared to have personal experience of buying any product.

Wait for product-

There is no instant buying in case of online shopping. You have to wait for delivery which may take minimum 2-3 days.

No assurance of quality-

One cannot be fully assured about the quality of the product purchasing online. Online product images are glorified many times. They may be vibrant, colorful, glossy in picture but in reality very dull and poor quality.

Product delivery issues-

Sometimes product does not deliver on time and it is very annoying for a consumer to wait in such cases.

Privacy and Security-

The major concern is that the privacy and security may compromise in online shopping. E-commerce sites, services, and payment gateways are prone to hack by hackers and consumer and trader may suffer huge loss. Customer's private information is hacked from their database which breaks the trust of consumers and they have financial or other losses too. Credit card frauds are also growing concern.

Misleading Advertisement-

To gain the profit and competing with others, many online trading sites use malpractices and misleading advertisements. It is the exploitation of consumer. There are misleading advertisements about quality, price, discounts, and services and so on.

Many cases of online false or misleading advertisement are reported in India. For Example, Flipkart's ad's claim "100% original products" and "Flipkart matlab bilkul pakka" was held not substantiated and misleading by exaggeration. Amazon kindle's claim of 'Unlimited Reading' is not substantiated in addition to not having any disclaimers. A limit of 10 books cannot be considered as an 'unlimited' offer.[4]

Defective goods and services-

[4] Vivek Pai, 'ASCI Calls Out Amazon, Flipkart, OLA, Quikr & Others For False Advertising'(Medianama ,18 August 2016) <www.medianama.com/2016/08/223-asci-false-advertising-may2016>acessed on 17 January 2021

Many of us may have experience that some online product or service is defective. Many times consumer is delivered with defective goods or services such as low quality, fault in products or services, less quantity, low standards and so on. Even some times product is totally different than pu rchased and consumer has to replace it.

Price manipulation-

Many e-commerce entities manipulate price to gain unreasonable profits. It also charge unjustified prices having regard to the prevailing market conditions or its essential nature and exploits the consumers.

Return and Refund-

Sometimes the return and refund policies are not flexible and in case any product is defective, to return that product consumer has to pay return charges which are also high. It is unnecessary financial burden and that is also for faulty product.

V. Significant Provisions under Consumer Protection Act 2019 in reference to E commerce-

The Consumer Protection Act, 2019 is enacted by the Central Legislature on 9th August 2019. It was enacted with an object as-to provide for protection of the interests of consumers and for the said purpose, to establish authorities for timely and effective administration and settlement of consumers' disputes and for matters connected therewith or incidental thereto.[5]

The Act has provided number of new significant provisions related to consumer protection to provide better protection to consumers and it has also widened its scope through inclusion of provisions related to E commerce. The consumer protection Act not only protects the normal offline consumers but the e-consumers as well. Some of important key provisions which provide better consumer protection in the new Act especially in reference to E commerce and E consumers can be discussed as follows

Consumer include E consumer-

The definition of consumer has been widened as compared to the old Act and the explanation to Sec. 2(7) (b). The explanation under said section states- the expression “buys any goods” or “hires or avails any services” includes offline or online transactions through electronic means or by teleshopping or direct selling or multi-level marketing.[6]

[5] Consumer Protection Act, 2019
[6] Consumer Protection Act, 2019, s.2(7)(b)

Thus, a consumer is a person that buys any goods or hires or avails any services for consideration but does not include a person who obtains such goods or avails such services for resale or for commercial purpose and e consumers are also added in the scope through explanation so consumer is now a person who buys goods or avails services both via offline or through online transactions and such transactions include the teleshopping, or direct selling or multilevel marketing. Further the Act provides definitions related to E commerce –

E commerce-

'e-commerce' means buying or selling of goods or services including digital products over digital or electronic network[7]

This definition not only provided a clear definition of e commerce but it also has widened the scope of definition of goods and services and now the digital products are also included therein.

Electronic service provider-

'electronic service provider' means a person who provides technologies or processes to enable a product seller to engage in advertising or selling goods or services to a consumer and includes any online market place or online auction sites[8]

The e-commerce entities like electronic service provider has been defined and brought within the scope of Consumer Protection Act through express provisions. The electronic service provider has not only been defined but it has also brought in the category of product sellers under Sec 2 (37).

Product Liability

The new concept of product liability has been introduced in the Act which means a responsibility of a product manufacturer or product seller, of any product or service, to compensate for any harm caused to a consumer by such defective product manufactured or sold or by deficiency in services relating thereto.[9]

So, the consumers including e consumers are entitled to compensation if they suffer any injury or harm from any defective product including the products bought through online shopping or deficiency in services including services hired through online transactions and also from defective digital products. The product liability is not only that of product manufacture but also of the product seller.

[7] Consumer Protection Act, 2019, s.2(16)
[8] Consumer Protection Act, 2019, s.2(17)

[9] Consumer Protection Act, 2019,s.2(34)

Powers of Central Government to take measures- under Sec94 and Sec 101(1)(zg), For the purposes of preventing unfair trade practices in e-commerce, direct selling and also to protect the interest and rights of consumers, the Central Government is empowered to take necessary measures and accordingly.

VI. Important Provisions under Consumer Protection (E commerce) Rules 2020-

The Consumer Protection E commerce Rules 2020' are framed by Central Government. The provisions are discussed as follows.

Scope and Applicability-

These rules apply to all goods and services bought or sold over digital or electronic network including digital products. It also applies to all models of e commerce including marketplace and inventory models of e commerce. It also covers all e commerce retail, including multichannel single brand retailers and single brand retailers in single or multiple formats. These rules apply to all forms of unfair trade practices across all models of e commerce.

E commerce entity means any person who owns, operates or manages digital or electronic facility or platform for electronic commerce but does not include a seller offering his goods or services for sale on a marketplace e commerce entity.[10]

Inventory E commerce entity means an e commerce entity which owns the inventory of goods or services and sells such goods and services directly to the consumers and shall include single brand retailers and multi-channel single brand retailers.[11]

Marketplace e commerce entity

An e commerce entity which provides an information technology platform on a digital or electronic network to facilitate transactions between buyers and sellers[12]

Platform means an online interface in the form of any software including a website or a part thereof and applications including mobile applications.[13]

User means any person who accesses or avails any computer resource of an e commerce entity.[14]

[10] Consumer Protection (E commerce) Rules,2020,s.3(b)
[11] Consumer Protection (E commerce) Rules,2020,s.3(f)

[12] Consumer Protection (E commerce) Rules,2020,s3(g)
[13]Consumer Protection (E commerce) Rules,2020,s.3(i)
[14] Consumer Protection (E commerce) Rules,2020,s.3(l)

The E commerce rules have placed certain duties and liabilities on e-commerce entities whether marketplace or inventory as well as upon sellers for better safeguard of consumers which are discussed as follows.

Duties of E commerce entities-

The following duties are placed upon e commerce entities-

1. It's mandatory for E commerce entity to be a company incorporated under Companies Act, 1956 or Companies Act 2013. If it's a foreign entity its mandatory to be a foreign company under clause 42 of Sec 2 of Companies Act 2013
2. The E commerce entity is under duty to appoint a nodal person of contact or an alternate designated functionary who is resident of India to ensure that there is compliance with provisions of Consumer Protection Act and other rules and regulations.
3. It is mandatory on part of E commerce entity to provide information in clear and accessible manner regarding legal name of the e commerce entity, its principal geographical address of its headquarters and all branches, name and other details of its website, contact details like e mail address, fax, landline, mobile numbers of customer care and the contact details of grievance officer.
4. E commerce entities are under duty to refrain from any unfair trade practices during the course of business as well as on its platform and in other matters.
5. The E commerce entities have to establish a grievance redress mechanism and they have to appoint a grievance officer for consumer grievance redressal. It is under duty to also furnish the name, contact details and designation of such officer on its platform.
6. The grievance officer is under duty to acknowledge the receipt of a consumer complaint with 48 hours. He also has to redress it within one month from the date of receipt of such complaint.
7. Where the e commerce entity imports goods or services for sale it has to furnish the information of the importer like name and other details from whom they purchase such goods or services. It has to furnish information of sellers also on such platform.
8. The E commerce entity is bound not to impose cancellation charges after confirmation of purchase unless it itself bears same charges for such cancellation.
9. The E commerce entity must record the consent of consumer in explicit and affirmative manner and not by pre-ticked automatic manner.
10. The e commerce entity has to refund payment for accepted refund request as per guidelines of RBI or other competent authorities in reasonable time in prescribed manner.
11. It is duty of e commerce entity not to manipulate price to gain unreasonable profit by imposing unjustified price on consumer.
12. It shall not make any arbitrary discrimination between consumers of same class.

Duties and Liabilities of E commerce marketplace entities-

The e commerce marketplace entity has to take an undertaking from the sellers which ensure that the descriptions, images, and other contents regarding goods or services are true, accurate and correct corresponding to appearance, nature, quality, purpose and other general features of such goods and services.

The e commerce marketplace entities have to furnish information on their platform related to the sellers of goods or services, their name of business, the geographical address, customer care number, ratings, or other feedbacks about such sellers which enables the consumers to make informed decisions. Such information is also to be furnished to consumers on request including all contact details, email address etc. in order to make it easy for consumers to communicate with the sellers directly in case of dispute for effective dispute resolution.

The marketplace entity should display the ticket number for each lodged complaint to enable consumer to track the status of complaint. Further it needs to furnish the details regarding the return like period within which replacement shall be done, refund policies, exchange, warranty and guarantee, delivery and shipment, like date of estimated delivery or shipment charges, modes of payment, grievance redressal mechanism etc. which enables consumers to make informed decisions.

It is bound to display information related to available payment methods, the security of payment methods, fees or charges to be paid by users, the procedure for cancellation of payments under, charge back options etc. along with the contact details of payment service provider. This is to reduce the risk of frauds or hacking the bank details etc.

The entity is bound to furnish the explanation of parameters which are significant individually and collectively regarding the basis of ranking of goods or services or of sellers etc. Thus there is mention of the ranking, the parameters like value for money, quality of material, delivery services, and other relevant parameters of particular good or service.

The entity should include in its terms and conditions the description in case there is differentiated treatment amongst goods or services or sellers It has to maintain records regarding identification of sellers who repeatedly offered goods, services which were previously removed or access to which disabled under Copyright Act, 1957, Trade Marks Act, 1999, or Information Technology Act 2000. It ensures that the products violating copyright or trade mark or other laws are not being offered to consumers without their knowledge.

Duties of sellers on marketplace

The sellers on marketplace entities are under duty to refrain from any unfair trade practices and from falsely representing themselves as consumers to post reviews about the goods or services. They are abstained from misrepresentation of features or qualities of any goods or services. The sellers shall not refuse to take back the goods or withdraw or discontinue any services which are purchased or agreed to be purchased or to refuse to refund the consideration that is paid, if they are defective or deficient or spurious or if such products or services are not of same characteristics or features as advertised or agreed to or if there is delay in delivery due to fault on part of such seller.

The sellers must have a prior written contract with e commerce marketplace entity for such sale or offer. They are bound to appoint a grievance officer for grievance redressal of consumers who is bound to acknowledge the receipt of any complaint within 48 hours and shall resolve the complaint within one month from such receipt. The sellers are required to provide the contact details, numbers, name, designation of grievance officer to consumers. Sellers are bound to provide to the e-commerce entity its legal name, principal geographic address of its headquarters and all branches, the name and details of its website, its e-mail address, customer care contact details such as fax, landline, and mobile numbers and where applicable, it's GSTIN and PAN details.

The sellers are bound to ensure that the advertisements of goods and services are consistent with the actual features, usages, conditions of goods or services and are not misleading. The sellers are under duty to furnish information on platform regarding all contractual information prescribed by law, total price of a single figure of any goods or services with breakup price, with compulsory and voluntary charges like delivery charges, postage and handling charges, conveyance charges, applicable taxes etc. Sellers shall furnish all mandatory notices and information required by laws, expiry date of goods, and other details of goods such as country of origin. It ensures that consumers can make informed decisions prior to purchase. Sellers shall share information related to name and details of importer, and guarantees related to the authenticity of the imported products; accurate information related to terms of exchange, returns, refund including costs of return shipping in a clear and accessible manner; details related to delivery and shipment guarantees or warranties etc.

Duties and liabilities of inventory e-commerce entities:

The inventory e commerce are bound to furnish the same information like sellers and marketplace entities , related to return, refund, warranty, guarantee, delivery and shipment, cost of return shipping, mode of payments grievance redressal mechanism, payment methods, security of payment methods etc and other relevant information . The entity is refrained from falsely representing itself as consumer to post reviews, refrained to misrepresent any features or qualities of goods or

services. It is refrained from misleading advertisement. It is bound to take back or withdraw any defective goods or deficient services or such goods or services when are different than as advertised. Other provisions are also applicable to inventory e commerce entities in same way as marketplace entities and sellers.

VII. Contravention-

The e commerce entities are liable for any violation of these rules provided under E commerce rules, Consumer Protection Act, 2019 as well as other relevant laws, under Consumer Protection Act 2019. The penalties include fine or imprisonment. The defaulter liable for false or misleading advertisement is liable for fine which may be up to 10 lakh rupees and further contravention it may be up to 50 lakh rupee or imprisonment which may be up to one year or in case of further contravention up to 3 years.

All these provisions have provided better safeguards for consumers. They have brought clarity and fairness in e commerce transactions. These will help consumers to make informed decisions along with better effective grievance redressal.

VIII. Shortcomings

There is still some ambiguity regarding various provisions. For example the sellers have to display the 'country of origin' but what's meant by 'country of origin' has not been clarified, also inventory e commerce entities are not required to display it. Also in case of prohibition of price manipulation there is no clarity as to what is 'unreasonable profit' or 'unjustified price'. There is no clear guidance about what is mean by 'arbitrary discrimination'. Also the penalties are not specified regarding the violation of rules and provisions.

IX. Conclusion

The E-commerce has no doubt a convenient, cost effective method of transactions for consumers to buy goods or services and to make online payments; it suffers from drawbacks like misleading advertisements, defective goods, deficient services, price manipulation, privacy and security issues in payment, unfair trade practices, issues related to return and refund policies, different goods than advertised etc. The Consumer Protection Act 2019 has made elaborate provisions in Act itself and in E commerce rules to curtail the menaces in e commerce system and has provided better safeguards to consumers by providing provisions for duties and liabilities on e-commerce entities and penalties in case of default. This has brought much clarity and fairness in the e commerce transactions. Also it will help for secure payment methods, and better and effective grievance redressal.

X. Suggestions

Some provisions of the Act need clarification and a guideline like what is ‘country of origin’, ‘unjustified price’, ‘arbitrary discrimination’ etc. proper guidance and directions are required. The specified penalties are to be mentioned.

ROLE OF INTELLECTUAL PROPERTY IN THE FASHION INDUSTRY: A LEGAL PERSPECTIVE

Pallabi Paul[1]

Abstract

The fashion industry is not only confined towards preparing designing and creativity, however, but it also covers all the activities for increasing the growth in the fashion industry like ad campaigns and marketing of products be it high fashion or will to achieve the competitive edge required for success.IPR plays a prominent role in the industry sectors like it ensures the ability of the creator to protect creations which include inventions, literary and artistic works, components of fashion designs, symbols, and images used in trade and commerce. Intellectual Property is related to the use of the intellect of humans to create anything novel or original. The fashion industry is related to IP intensive industry, persistently producing and monetarily misusing inventive thoughts and development. In this paper, the author has shed light on different types of Intellectual Property and their applicability to the Industry related to the fashion world along with the development in the laws related to Indian Intellectual Property for securing the creativity of various products in the Fashion Industry. Despite the innumerable advantage of IP, it is usually misjudged. Fashion design is a type of creativity devoted to the formation of dress and another way of life embellishments and to work as a designer, one should have an aesthetic and innovative character and have a decent visual creative mind and placed their thoughts into pieces of clothing and the creativity are required to protect. Highlighting the leading case of Star Athletica, LLC v Varsity Brands, Inc, the paper focuses on the effect of 3D printing and artificial intelligence (AI) on the fashion industry and its growth.

Introduction

The fashion industry doesn't revolve around clothing's and apparel and its sale in the market, but they devote towards the intellect and innovative ideas to yield something creative, novel in the form of fashion design and other products apart from designer garments like footwear, jewelry, handbags, and high fashion designers product. Thus, other than the high designer garments, these products are part of the fashion industry. The fashion industries

[1] Student, Dept. of Law, Assam University, Silchar Assam

are associawith several halves of works like manufacturing, designing, retailing, advertising, promotion before the final sale of the products in the market[2]With the advancement in technology, emerges a significant expansion ofthe fashion industry and now requires creativity to be protected from getting pirated.[3]Fashion design, are in the state of low IP equilibrium" which implies that due to the sophisticated software technology, it's become easier to copy the design of the original creator, and hence IP protection, is considered as a driving force behind fashion innovation. Piracy will affect the integrity and authenticity of the fashion industry's productivity. These days, the fashion industry has evolved in such a way that now a product is manufactured in one nation, designed in another, finally comes in the market for sale in other and It can be estimated from observation of by the increase in numbers of events with regards to promotion and advertisement of fashion designs by brands within the period from 1 in 2004 to 5 in 2013.[4]Based on the analysis of the Associated Chambers of Commerce and Industry of India (ASSOCHAM), the designer apparel industry at the local level in India, with a budget of around Rs. 720 crore and has reported a compounded annual growth rate (CAGR) of about 40% in 2012, which may increase further in near future with a worth of Rs. 11,000 crore.[5]

How are IP issues affecting the fashion industry?

The IPR and fashion industry are embedded with each other. The Intellectual Property Rights laws play a vital role In the proliferation of the fashion industry where the law used to protect the creator's rights and increase the encouragement of the creator to invest his ideas in the form of designs which are considered as fashions are the intellectual creations of an individual**.**[6]IPR recognizes certain rights of the originator by granting him an exclusive right to use, exploit commercially by receiving monetary benefits. And hence the present legal system is working for a decade to enhance creativity by granting legal recognition to come up with novel ideas that may ultimately fuel the growth of an economy**.** In absence of legislation to protect creativity effectively, will lead to drastic loss to our country, and there will be

[2] Shishir Tiwari, Intellectual Property Rights Protection of Fashion Design in India: A Panoramic View, (July 6,2016). Available at SSRN: https://ssrn.com/abstract=2805346 or http://dx.doi.org/10.2139/ssrn.2805346(assessed 12th Feb 2021)
[3] Ronojoy Basu, FASHION, IPR & THE EMERGING DESIGNER-IP Protection and Contractual Safeguards for Emerging Designers and Small Fashion Firms
[4] ibid
[5] Pranjal Shirwaikar, Fashion Copying and Design of the Law, Journal of Intellectual Property Rights, Vol 14, March 2009, pp 113-121
[6] ibid

fewer emerging creators and people who will not come forward to innovate, and no new creations will be created.[7]

Legal rights of the fashion designer which encourages innovation is -

(i)Protection: The IPR laws acts as protector If the creator by taking legal action against those who take wrongful benefit from copying or using textile or product in absence of authorization; and

(ii)Commercial exploitation: The designs or innovation creations are commercially exploited by people once they agree to receive licensing for the use of the same.[8]

IP rights not particularly concerns for the protection against copying and piracy. However, they are considered as the law which performs a more subtle function, recognizing the maker of designs. By receiving a methodology more much the same as that taken inside the media and media outlets, style brands can arrive at that next degree of complexity whereby they are deliberately dealing with their IP rights particularly from their business activities.[9]

Piracy, Crimes, and Redressal

Fashion piracy, when restricted to unreliable administrators, is currently out of the storage rooms and making a significant tempest in the abounding universe of haute couture. The turnover of the marked instant industry is Rs 2,500 crore and is developing at 30%. With the increase in piracy cases in India, many entrepreneurs have opened their shops in basements and garages, with a presumption that it is difficult to create innovative content and form a design and rather believed to copy designs from branded designers. Although copying and pirated works face criticism while still it's acceded because of ‘homage’, ‘dedication’, ‘inspiration’, and many times the no legal action is taken for the infringement of the rights of the original designers.[10]The operation of the fashion industry requires a large investment, constant innovation, and production within short periods continually with or without the grant of protection of IPR**.** Piracy is in order words refers to the unlawful reproduction or reproduction, printing or distribution of any content which is the original work of another

[7] Christine Cox and Jennifer Jenkins, Between the Seams, A Fertile Commons: An Overview of the Relationship Between Fashion and Intellectual Property

[8] John Zarocostas,The role of IP rights in the fashion business: a US perspective, WIPO Magazine, https://www.wipo.int/wipo_magazine/en/2018/04/article_0006.html(assessed 12th Feb 2021)

[9] ibid

[10] ibid

person and the creator was granted with protection under the laws related to copyright, patent, or trademark.

[11]

Basically, the unauthorized copying is the attributes of piracy. This piracy or copying in the industry is all about copying any design in apparent, footwear, customers, bags, etc either partly or wholesome, or copying any logo or name or anything of the brand. Fashion Design Piracy(FDP) includes unapproved duplicating of unique design plans.[12]Also, for the most part, it can be categorized as one of the two after classes: (1) knockoffs and (2) fake. The knockoff is a duplicate or impersonation of a person or thing well known and it is created wrongfully without a license.In the fashion world, a knockoff is a nearby duplicate of the first style configuration, copying its components, yet is sold under a name unique about the mark of the first plan. Accordingly, it isn't sold trying to pass as the first. Knockoffs are planned to duplicate the first plan almost line for line yet with another planner's name attached.[13]A line-for-line duplicate is an almost indistinguishable impersonation of a unique plan. Rather than knockoff, a fake is a duplicate of the first style configuration just as the brand logo or name of that plan. Here, the aim is to misdirect purchasers of the attire's actual substance and beginning both.[14]

What is going on in the market?

Now the piracy or copying of design has increased in the market in such a way that even some of the reputed industries also used to copy the design of others, where the innovative creation of the creator and his rights are infringed, which leads to the replica is sold at less price in the market, and where any product is available at less price, many people would not prefer to purchase something expensive.[15]

The plight of the emerging designer

Although it's true that with the technology are developing to copy the content or any design which has been made public piracy is somehow accepted and there is no strong

[11] Kal Raustiala and Christopher Sprigman, The Piracy Paradox: Innovation and Intellectual Property in Fashion Design, Virginia Law Review, Vol. 92, No. 8 (Dec. 2006), pp. 1687-1777 (91 pages)
[12] Rohan Gandhi, Role of Intellectual Property in the Fashion Industry,https://www.google.com/amp/s/lexforti.com/legal-news/role-of-intellectual-property-in-the-fashion-industry/%3famp(assessed 12th Feb 2021)
[13] ibid
[14] ibid
[15] Piracy fuels fashion industry, https://www.nytimes.com/roomfordebate/2014/09/07/who-owns-fashion/piracy-fuels-the-fashion-industry(assessed 12th Feb 2021)

mechanism to redress the grievances of the creator, nowadays the multinational companies which deal in the apparel industry and other products gain more advantages from copying as compared to the budding designers.[16]With the arrival of sophisticated technology, it has enhanced the pace of copying in such a manner that copies or counterfeit products are introduced in the market before originals which brought difficulty for the growing fashion designers to bring new innovative creations in the form of design and to beat the copyists**.** To overcome this issue, several fashion industries have initiated to assist young designers by offering money and mentoring.[17]Earlier no prior legislation or policy was made to regulate the piracy issue and rights of fashion designers, however, after that CFDA (Council of Fashion Designers of America), which is one of the biggest trade organization for fashion and accessories designers in the US has attempted to reform intellectual property law to protect fashion design, offers grants, prizes, and education programs to promising emerging designers.[18]The current monetary truth is that these endeavors may not be sufficient. Youthful originators are battling to remain in business as requests are dropped or returned.[19]One frequency of replicating costing a significant deal could e father.[20]

The Fashion Foundation of India (FFI) was set up during 2008-2009 in India with association with brand names throughout the country as founding members. The organization used to work with macro and micro issues with regards to the fashion industry and they endeavors to provide soft loans and grants based on business proposals made by the designers/agencies, commissioning studies analysis area, along with legal assistance on the matters related to IP, contracts, arbitration, etc**.**[21]However, questions have been brought about its viability up considering the immaterial commitment of the Fashion Design Council of India (FDCI).[22]towards handling style copyists or forcefully pushing for changes,

[16] Supra Note - 2
[17] ibid
[18] Felix Salmon, Susan Scafidi on Copyrighting Fashion¸ UPSTART BUSINESS JOURNAL, (Jan.15, 2021, 5:00 PM)http://upstart.bizjournals.com/views/blogs/market-movers/2007/09/19/susan-scafidi-on-copyrighting-fashion.html?page=all(assessed 12th Feb 2021)
[19] Eric Wilson, The Make or Break Season, THE NEW YORK TIMES, FASHION & STYLE, (Jan 15, 2021, 4:15 PM) http://www.nytimes.com/2009/02/05/fashion/05SMALL.html?pagewanted=all(assessed 12th Feb 2021)
[20] Education and Professional Development, FASHION FOUNDATION OF INDIA (Jan. 18, 2021, 4:15 PM) www. fashionfoundation. in
[21] ibid

[22] Emily Gyben, Knockoffs and Counterfeits: What's the Difference? Prof. Susan Scafidi in Fashion etc., FORDHAM UNIVERSITY (Jan. 15, 2021, 3.30 PM) http://law.fordham.edu/faculty/22387.htm(assessed 12th Feb 2021)

authoritative and something else. Tarun Tahiliani, one of the nation's style doyens, has noticed: "We have attempted to death, however the structure (at FDCI) was simply not permitting us to get fundamental changes that might have been extraordinary for the business. However, at FFI, the structure would work in a lithe way that would allow us to take snappy choices.[23]Emerging style planners in India have battles like their Western partners regarding seeing impersonations of their manifestations being auctions directly off the roads. One of the issues adding to the high theft of originator garments is the emotional ascent in style for a long time in India. The more the style weeks, the more the openness, the more the odds of plans being replicated. Also, most Indian fashioners are very careless about looking for copyright assurance in light of the time and cash involved.[24]

The rise in fashion-related IP litigation about social media

To advertise and increase promotion of their products to attract the attention of the consumers, many fashion designing brands used to promote the products by using the content of other brands in the form of posts without their prior consent to do so which less to infringement of the rights of the original creator and lead to challenging the right related to copyright**.[25]**Besides this, there are instances where the trademark of any reputed brand is hijacked and misused where the attackers register it as their domain name illegally. In 2017, a trademark lawsuit was filed by US sports apparel manufacturer New Balance against China after that The Suzhou Intermediate People's Court asked the three Chinese shoemakers to compensate by paying more than RMB 10 million (around USD 1.5 million) to New Balance for copying its signature slanted "N" trademark.[26]While small by international standards, the damages are reported to be among the highest to have ever been awarded to a foreign company in a trademark dispute in China.

Fashion Design's Protection and regulations under the Intellectual Property Rights Regime

[23] Schmidt Rocky, Designer law: Fashioning a remedy for design piracy, UCLA Law Review, 30 (1983) 861; Mencken Jennifer, A design for the copyright of fashion, Boston College Intellectual Property & Technology Forum, 1997, F. 121201.
[24] ibid
[25] ibid
[26] ibid

The legislation of Europe and the US recognizes the rights of the original creator of content of apparel and it's related products by conferring design rights, however, Indian legislation also guarantees the rights of designers as the Fashion Foundation of India (FFI) has been composed of numbers of top designer from India who are in desire to protect IP rights against rampant copying, 'referencing' and 'inspiration'. It along with a legal cell look after all relevant areas where research is required, further with the help of its Research and Analysis Cell**,** analyzes different aspects of the fashion industry**.** A legal cell is constituted which indulges in matters like IPR, licensing, contracts, and arbitration of the design house. Further, the design houses are permitted to apply for membership of the Foundation and a business representative nominated by each design house will be a member of the Foundation. Certain groups of people acting as judge and connected to design will audit and examine every participation application.[27]One can unmistakably plan the likenesses between the objects of the Fashion Originator's Guild in the USA and the Fashion industry of India. The current lawful system gives a fascinating mode to secure the inventiveness in design. The Indian fashion industry is as of now esteemed at $67.6 million and is ready to develop to $187.7 million by 2012.Indian fashioners have vigorously depended on old conventional and native plans to make articles of clothing.[28]Fashioners keep on utilizing old and native craftsmanship and specialty to either make or adorn their garments.'Indian designers have perceived the requirements of the worldwide market and are working likewise. With the smart utilization of embellishments, native procedures, and art — the Indianness unblemished — they are making present-day outfits, which are getting a worldwide response. A considerable number of style fashioners depend on native and customary specialties, coloring, block-printing, and weaving strategies to make new plans and structures.28 Indian planners and couture have depended and acquired monstrously from old techniques and methods of attire and culture. Old conventional and native craftsmanship that was once restricted to particular districts distinguished by the skill of a bunch of individuals is currently a piece of the ramp. Various strategies, for example, coloring, block-printing, weaving, have been utilized to make the fundamental texture. Native strategies, for example, chikan Kari, phulkari, Kantha, and different types of weaving and slicing have been utilized to make clothing plans and restore old works of art. Nonetheless, clashes will undoubtedly emerge

[27] Sayali Diwadkar, India: Role Of IPR In The Fashion Industry,https://www.mondaq.com/india/trademark/704378/role-of-ipr-in-the-fashion-industry#:~:text=India%3A%20Role%20Of%20IPR%20In%20The%20Fashion%20Industry&text=Each%20year%20the%20fashion%20hub,product%20features%20or%20a%20print(assessed 12th Feb 2021)
[28] ibid

where antiquated fine arts and painstaking work remain outside the domain of IPR. It would coherently follow that plans that essentially depend on such types of workmanship and handiwork normally stay outside the domain of a protected innovation system. It is past the explanation of equity to give IPR to subsidiary natural products dependent on old and customary information, where the foundations of such information and scholarly manifestations remain past property rights. The licensed innovation system in India accommodates assurance under the Designs Act 2000, the Copyright Act, 1957, and the Geographical Indications of Goods (Registration and Prohibition) Act, 1999. Even though there is by all accounts three unmistakable enactments, that ensure three particular qualities simultaneously and a lifetime of the style attire or the frill. The creative work in the portrayals of the plans (when they are diminished to a material substantial medium) is secured under the Copyright Act 1957.[29]The Designs Act 2000, is so drafted to allow insurance of the non-practical parts of an item, having visual allure.

Intellectual Property laws and the Fashion industry

Trademark in the Fashion industry

Trademark, which is a visual mark used to distinguish the goods and products of one business from another. In the fashion industry, each brand has it's logo or label which represents its unique services and products, trademarks are there may be in the form of the logo of the apparel, or clothes, which seeks to protect the rights of fashion designers by its name and distinctiveness and distinguish the product from its competitors.[30]With the help of Trademark law, it has introduced trade dress i.e. the total image of the product including size, shape, color or color combinations, texture, graphics, or even particular sales techniques. Some of the examples are - Burberry has been granted rights under trademark where both its name "Burberry" and the Burberry check pattern are protected. Again, in the case of Louis Vuitton, the 'LV' logo is protected under trademark as a part of the design. Similarly, Pickwick is well known for its casual fashion wear for youngsters which is sold across

[29] Grail Research (2009), The Global Fashion Industry – Growth in Emerging Markets (Research Report), 1-22, availableat, <http://www.grailresearch.com/pdf/ContenPodsPdf/Global_Fashion_Industry_Growth_in_Emerging_Markets.pdf>(assessed 12th Feb 2021)

[30] Shamnad Basheer (2007), “The Piracy Paradox: "Fashionable" IP”, available at, <http://spicyip.com/2007/09/piracy-paradox-fashionable-ip.html> (assessed 12th Feb 2021)

Europe.[31]The trademark of the fashion brand consists of a teenage guy with a trendy hairstyle**.** From that point, Teenagers started seeing the Pickwick logo as stylish and are eager to pay extra for garments bearing its trademark.[32]

Copyright

Copyright is a component of IPR that recognizes all the literary and artistic work and its related aspects, moreover, it allows all the work which are already published and can further use. There are provisions under the Copyright Act, 1957 in India which ensures that the individual who is the creator is entitled to certain rights during the lifetime of the artist along with further 60 years after he passes away. It assumes a significant job in inspiring a creator and subsequently guaranteeing that the illicit utilization of his innovativeness or expertise isn't gotten.[33]

Trade secret

It alludes to the center ideas by the utilization of programming apparatuses for fashion design, computer, programming based plans of action, and coordinations on the board of the whole worth chain. Through the assurance of data by IP business concerns can focus on a grounded market position and control its piece of the overall industry, net revenues, separation, advancement in this manner maintaining a strategic distance from the danger of IP encroachment. IP assurance of resources makes a general picture according to the speculator and customer.[34]For example -An improved data innovation framework has been picked by Zara to abbreviate its creation cycle to a simple 30 days while that of its rivals range from 4 to a year. Additionally, a cutting edge dispersion framework, for certain 200 kilometers of underground follows and more than 400 chutes, guarantees that the completed things are transported and show up in stores within 48 hours. Shirtsdotnet is an attire stage that offers clients a choice to plan and request clothing straightforwardly from its virtual shop.

[31] Akansha Chopra and Rounak Biswas, IPR laws applicable to the fashion industry in India, leader, https://www.google.com/amp/s/blog.ipleaders.in/ipr-laws-applicable-to-fashion-industry/amp/(assessed 12th Feb 2021)
[32] ibid
[33] Dr. M.K.Bhandari, Law Relating to Intellectual Property Rights,28 CLP(5th edn, 2019)
[34] id at 7

Restrictive programming which is ensured as a proprietary advantage has been embraced to give mass customization garments arrangements.[35]

Patents

All the innovative ideas which can produce technical products by the inventor, or anything in the form of fabric or any material, design are eligible for patent protection. The Danish biotech company, Novozymes has discovered an enzyme and microorganisms known as cellulose which is used for the protection of fabrics. This eliminates a portion of the indigo color from the denim to give a rugged look.[36]

Effect of 3D printing and artificial intelligence (AI) on the fashion industry and its growth.

With the use of AI, now it has affected, in such a manner that now it became easier to copy 3D printing and to reproduce the same infringing the copyright-protected patterns and trademarks. For example, the logos, labels of any organization are copied without consent in a 3D version. However, it's fascinating right now is blockchain and its expected both to help right holders in the account and dealing with their IP rights and to battle against fakes. Handling fake products, especially on the web, is an exorbitant, tedious, and ceaseless cycle for brands.[37]

Star Athletica, LLC v Varsity Brands, Inc

Star Athletic, LLC v Varsity Brands, Inc. was a milestone case that went under the steady gaze of the Supreme Court in 2017. The case focused on the protectability of cheerleading outfits. In particular, it analyzed whether certain inventive components of the plan of a team promoter's uniform –, for example, the stripes of a chevron – could be secured under US copyright law. At the end of the day, could these components be isolated explicitly or adroitly without removing the reason for the plan, specifically to be a cheerleading uniform? In its choice, the Supreme Court reiterated the norm for distinguishableness, saying

[35] Chadha & Chadha Intellectual Property Law Firm, Significance of intellectual property in the fashion industry, https://www.lexology.com/library/detail.aspx?g=3011b365-d004-402f-8a62-1a52265787b0(assessed 12th Feb 2021)

[36] ibid

[37] John Zarocostas, freelance journalist, The role of IP rights in the fashion business: a US perspective, August 2018

that, when all is said in done terms, certain imaginative components – regardless of whether two-dimensional or three-dimensional – of a piece of clothing might be ensured by copyright law. Nonetheless, it would not address the protectability of, or the degree of innovativeness characteristic in, the particular garbs being referred to. The case needs to return to the lower court to decide if the cheerleading components were adequately unique to warrant insurance. While it isn't yet clear what the pragmatic effect of the choice will be on the US-style industry, it offers fashioners some desire for having the option to utilize copyright law to put forth a defense for safeguarding probably some inventive parts of their articles of clothing.[38]

Judicial trends in the fashion industry

In the case of **Yves Saint Laurent v Ralph Lauren,**[39]the Court ordered Ralph Lauren to pay compensation of about $385,000 for copying and reproducing a tuxedo dress which was designed by Yves Saint Laurent.

Ritika Apparels v BIBA[40]

In this case, the plaintiff filed a suit against the opposite party on the allegation that the design of the creator was copied without prior authorization, reproduced, and sold in their name in illegal intention to gain profit which violates the copyright granted to the plaintiff. On the other side, the defendant took the defense of Section 15(2) of the Copyright Act, 1957 and argued that the plaintiff does not own the copyright to the production anymore as the maximum duration of copyright has exceeded more than fifty numbers and thus he has not infringed the right of the original right owners. However, similarly, the design does not receive protection under the Designs Act, and hence it could not be recognized other than producing products having the same design less than fifty numbers of times**.** However, the court held that the defendant was not liable and due to lack of proper knowledge regarding IPR, of the designer as the design is registered under the Designs Act, 2000 and hence entitled to receive protection for 15 years. Yet, maybe the fashioner needed to save a restraining infrastructure on a similar plan for a more drawn out period and along these lines

[38] 137 S. Ct. 1002 (2017)

[39] Societe Yves Saint Laurent Couture SA v Societe Louis Dreyfus Retail Management SA [1994] E.C.C. 512 (Trib. Comm. (Paris).

[40] Under Section 15(2) of the Copyright Act, 1957, IA No. 13045/2011 (under Order VII Rule 11 CPC filed by the defendant) & CS (OS) No. 182/2011

utilized the copyright law which later on was betrayed her in this manner prompting the turnedbecoming liberated from any liabilities.

Christian Louboutin v Mr. Pawan Kumar & Ors[41]

In this case, a major brand renowned for its profoundly adapted creator shoes managed the selling of counterfeit items at a lesser price causing misfortune both to the brand name and to the monetary coffers of the organization. Christian Louboutin's Red Sole shoes are very mainstream among celebrities and the red shaded high obeyed shoes are a significant fury among the clients who plan to duplicate their number one big name's design sense and style. However as referenced before as well, the first items are exceptionally estimated, in this way keeping the items out of the span of the greater part of the clients. Louboutin's image has set up itself as a celebrated brand and a world chief by methods for utilization of media and TV. Louboutin's shoes are known by their unmistakable and trademark red-hued soles which are regular in the entirety of his manifestations and are promoted through explicit channels and stores (Louboutin has 120 such stores the whole way across the world and two such stores are there in India, one in Mumbai and other being in Delhi). Louboutin's items are secured under the brand name laws and the altruism and notoriety of the brand existed even before the brand's proper passage into the Indian market. The litigants began showcasing fakes of the much commended red bottom shoe, in any case, with various shading plans where the bottoms were red however different parts came in various shading schemes. The offended party, Christian Louboutin moved to the court looking for a perpetual order and remuneration claims from the two stores (Kamal Footwear and Adara Steps) selling fake results of Red Sole Shoes. The court in its judgment held the litigants subject to pay a complete amount of Rs. 10.72 Lakhs, while they were injuncted for all time from selling the fakes once more. The Judge in its judgment announced Christian Louboutin as a notable imprint, a much-pursued tag for any brand proprietor. The encroachment of Louboutin's imprint and effective indictment of the respondent shoe storekeepers are the best instances of how a creator or a brand proprietor needs to ensure their brand name.

Recommendation and Suggestions

[41] High Court of Delhi, CS (COMM) No. 714/2016.

Thinking about the issues in question, one might have the option to comprehend that even though there are legitimate insurances accessible, more often than not the fashioners are to blame. It is no uncertainty genuine that the lawful assurance concerning the style business is minimal weak, by and by, the architects additionally should be careful about their manifestations and they need to plan in like manner. Following are a couple of methods of battling the issue, which is as per the following- Expanding the edge furthest reaches of the items created by mechanical application from 50 to more number under the Copyright Act – a number proportionate with the thought of the rising populace and the way that the machine creation is stylish these days.[42]

Revising the laws to make the buyer subject as well, aside from the merchant of the fakes. The laws should be made in consonance with the global principles like that of France.[43]

Making a fixed level of benefit of the infringer organization to be taken care of as payor punishment, much like the EU GDPR punishment arrangements.

Upholding IPR laws in a more tough manner maybe by forcing criminal accusations too on the forgers separated from the pay which is as of now stylish today, so that lifting of plans are controlled to a great extent if not completely forestalled.

Sharpening the Designers about the need of securing their IP in the right manner so future inconveniences can be deflected.

Sharpening and making the public mindful of the fake products predominant on the lookout and the terrible sides of utilizing them.[44]

Conclusion

The design business has fundamentally developed in the new years, controlled by the advancement further reinforced by powerful execution and utilization of laws. In any case, it has been seen that the planners more often than not neglect to secure their IP utilizing the lawful course. We have seen such a pattern in Ritika Apparels case and the People Tree situation where because of the absence of legitimate insurance the respondents went without any penalty. Simultaneously, Christian Louboutin won perpetual directive against the forgers and got made up for the misfortune. The thing that matters is a direct result of the legitimate

[42] IP and Business: Intellectual Property in the Fashion Industry, WIPO MAG, (Aug.26, 2014, 2:00PM)http://www.wipo.int/wipo_magazine/en/2005/03/article_0009.html(assessed 12th Feb 2021)
[43] ibid
[44] ibid

IP techniques and earlier enrollment of the imprint which gave the brand an additional preferred position in the lawful procedures. While the facts demonstrate that it is practically difficult to annihilate duplicating and keeping others from replicating if the creation is ensured in a correct manner it lessens the odds of the misfortune by diminishing the harm. Hence it is of high significance that the makers of IP ought to consistently stay alert and should attempt to get the correct security for their creation. Additionally, the public authority needs to contemplate the new pattern of duplicating and pass a sui generis law explicitly material to the style business, to secure the IP of the nation and by and large to fortify the nation's economy.

DIGITAL ERA AND COPYRIGHT ISSUES: AN ANALYSIS

Dr Sujatha Patil[1]

Abstract

Advancement of science and technology really changed overall perspective of human toward the life. Every day new technologies keep coming and making our life more easy and comfortable. Even the digital technology in the present era is playing very significant role and it's been extensively used to store, record and disseminate information in the digital platform. The readily availability of information on digital platform makes more prone to IP violations. The major challenges that need to be addressed are Copyright issues. Easy access to the material that is available on internet has really created the greater concern about infringement of copyrights of the owners/creators.

An attempt has made in the present paper, in understanding the issues and challenges faced by copyright owners due to digitization and followed by the suggestions to protect the copyrights of owners/authors and at the same time making the work accessible to the public for research and teaching purposes by using the concept called 'Fair Use Doctrine under Indian Copyright Act 1957'. In addition to this, the paper will also address about the remedies available for infringement of copyright in digital domain and how for these remedies actually serves the purpose.

Introduction

Advancement of Digital Technology has been one of the great and useful creations of the human mind. Really it has opened gates to wide range of possibilities in various areas like media, entertainment, advertisement and education too. With rapid spread of digital technology and people becoming techno savvy, it has helped the people to get inclined towards E-learning. For example, when it comes to literary work under copyright, wherein we can notice the millions of books and research papers, journals etc., are assembled under digital platform and these digital libraries are catering as a research tool of historic significance to number of students, teachers and researchers. Digitization helps in

[1] Dr. Sujatha S. Patil, Associate Professor & Principal of Law, School of Business & Law

overcoming the barriers that we face physically in terms of time, money, space and availability of books etc. These are the few best part of digitization.

In addition to best part of the digitization, there were major copyright issues and challenge that needs to be addressed. Easy access to information and materials available on the internet created a great concern in protecting the rights of the copyright owner from infringement. IPR (Intellectual Property Rights) broadly classified into two rights, a) industrial property and b) copyright and other related rights. Copyright is one such important IP right, which deals with the rights of the creator for the works like literary, artistic, drama, music, film, sound recording computer program etc. Digitization considerable made all these works very much easy to copy, replicate and sell the works without authorization copyright owner and which in turn the detection of such infringement becomes difficult. This has posed a great threat to the right of the copyright owners and creators.[2] This paper will address all the issues, challenges and the remedies available to overcome these situations and followed by suggestions to balance the present scenario.

Digitization and Its Challenges

In the present technological era, we can notice lot of initiatives with regard to digitization have been taking place globally in order to preserve the data and also to overcome the barriers of time and space. Digitization is nothing but scanning the books, manuscripts, historical records, photographs etc. From the middle of 1900s, thousands of libraries and other online data sources started scanning their data collections, in order to make the work available on the internet.

Challenges:

1. The creation of telecommunications and internet across the country has created major issue to the digitization.
2. Physical environment like sitting in the library, meeting the people and discussing on a table is completing missing in of case of Digital library. In reality what we notice that, people are very much comfortable and would prefer to read from printed material rather than reading through computer screen. This is due to lack awareness of usage

[2] Nehal Wagle, Copyright in Digital Era, https://blog.ipleaders.in/copyright-digital- accessed 20th Jan 2021

of technology, which in turn the people are reluctant to study the material in digitized form.[3]

3. Another factor which will ponder a lot is of expenses. The initial cost of digitization can be quite high.
4. The technical issues that we encounter in the digitization process, needs to handled by the people who are expertise. The non-availability of well-trained personnel, lack of management support, outdated software and hardware are major issues.
5. Another challenge that may be faced is that the publishers who want to provide E-book will suffer if in case copyright books are digitized
6. Authors/owners of creative work fears that the market of their creative work will be affected if their works are digitized and are freely available.[4]

Copyright

Copyright (or author's right) is a legal term used to describe the rights that creators have over their literary and artistic works.[5] Only human beings are capable of creativity. They can be authors, composers, artists and designers for creating their original works[6]. The works which fall within the copyright protection are as follows:

1. Literary works such as novels, poems, plays, reference works, stories including fiction and non fictions, newspaper articles
2. Films, musical compositions and choreography
3. Computer programs, database
4. Artistic works includes the work having artistic character such as drawings, painting, photographs and sculpture etc. It also includes advertisements, maps and technical drawings[7]

Copyright law aims to balance the interest of those who create the work/content with the public interest in having widest possible access to that work/content.[8]

---

[3] Dr. Manoj Kumar Verma, Nitesh Kumar Verma, "Concept of Hybrid, Digital and Virtual Library: A Professional Approach", https://www.academia.edu/11404741/Concept_of_Hybrid_Digital_and_Virtual_Library_A_Professional_Approach, accessed 28th March 2021

[4] Heena Dhyani, "Digitisation of Libraries and the Copyright Issues", The GNLU Law Review, Vol. 5, (2018), p.94

[5] Ibid

[6] Dr. G.B. Reddy, Intellectual Property Rights and the Law, (Gogia Law Agency) 69

[7] Heena Dhyani, "Digitisation of Libraries and the Copyright Issues", The GNLU Law Review, vol 5 2018, p 94

[8] Copyright, https://www.wipo.int/copyright/en/, accessed 24th March 2021

Challenges faced by Copyright in Digital Era

Since inception of digital technology, copyright law has responded to its changes, Today the changes that are grabbing all the headlines relates to digital technology and digital communications networks, such as internet, computer, multimedia, social media. These technologies are promising and potentially harmful to varies parties interested in the use and exploitation of works of authorship-from books and music to film and web pages. Let us see few of the platforms creating a impediment to copyright works.

1. Internet:

Since form long time, internet has been one of the major threats to copyright. The information that is easily accessible on internet has varying degree of copyright protection. The copyright work that is available on internet includes e-books, e-journals, e-magazine, news images, screen play, videos etc. In this technological era, the information that is available on internet is like ocean but the greater challenge is, to determine I mean to find whether the work is duplicate or protected under the Copyright Act. It is always common myth that the freely accessible information through internet on public domain can be copied freely. As per the law, until the information has been made available by the government, or the term of copyright got expired, no one is having right to copy it.

2. Computer Software

It is nothing but the collection of computer programs, procedure, documentation that perform tasks on a computer system. As we are noticing rapidly that software piracy is one of major reasons of copyright infringement. It involves unauthorized copying, distributing of copyrighted software, Copying of software programs using CD-R technology etc.[9]

3. Social Media

In the present days social media platform plays important role and hold very prominent position in connection the people across the world. These platforms help in sharing the works which may be copyrighted. The practices of sharing the information, materials such as images, videos, photos on social media platform has resulted in gross infringement of copyright. The biggest myth of the people is that, whatever material they share on the social

[9] Nehal Wagle, Copyright in Digital Era, https://blog.ipleaders.in/copyright-digital- accessed 28th March 2021

media is completely free. This ignorance in turn leads to major cause of infirmness. The different mode of copyright violation on social media platform is as follows:

1. Re-posting or sharing of works which was protected under copyright law
2. Using the content available on platform of someone else without permission.

4. Multimedia Work.

Multimedia is such a concept which is extensively wide and encompass within it different categories of materials like information, sounds, audio & video, live video speech, picture and images etc. Even though the protection of copyright is also available to multimedia but the problem is that, under the ambit of multimedia the creators and owners will get variety of rights, due to which protection of copyright will become difficult.

Fair Dealing in Digital Era

Well, before we discuss about how the concept of fair dealing plays as an exception to infringement in digital era. Let us have an idea about the concept of fair of dealing. It is known fact that, any person who uses copyright work without permission of owner is considered as infringement. However, there are certain acts which won't fall under infringement even though it is done by a person order than owner. This is what we call it as exceptions to general rule.

The purpose of recognizing these exceptions is to enable reproduction of work for public purposes, for encouragement of private study and to carry out research and promotion of education.[10] Section 52 of Indian Copyright Act, 1957 provides certain rights to content users including researchers to access materials. Section 52(1) sub clauses (a) to (zc) provides exceptions to the exclusive rights. However, even the user needs to ensure that it won't leads to infringement and should also respect the rights of the owners.[11]

The protection given to the owners and creator of copyright work must in conformity with public rights. The main purpose of Section 52 is to provide the freedom of speech and express as enshrined under Art 19(1) of the constitution of India so that the work related to research, private study, review, criticism and reporting current events could be protected.[12]

[10] Dr B L Wadehra, Law Relating to Intellectual Property, 5th ed,(Lexis Nexis), 2018, p 328
[11] Heena Dhyani, "Digitisation of Libraries and the Copyright Issues", The GNLU Law Review, vol 5 2018, p 96
[12] P. Narayana, Intellectual Propeerty Law, Kolkata: Eastern Law House

According to Art 9(2) of Berne Convention 1883 "It shall be the matter of legislation in the countries of the union to permit the reproduction of such work in certain cases, provided the reproduction of such does not conflict with normal exploitation of the work and does not legitimate the interest of the author".[13] Even Art 13 of TRIPS Agreement states "Members shall confine limitations or exceptions to exclusive rights to certain special cases which do not conflict with a normal exploitation of the work and do not unreasonably prejudice the legitimate interest of the right holder."[14] If we look at in each and every country we find different laws on copyright exceptions. The copyright exceptions in USA is called as 'fair use', in UK it is called as 'fair deal', in European Union Directive is used as compulsory and optional exceptions. In India under Section 52 of Copyright Act provides exceptions to exclusive rights.[15]

The acts which shall not be considered as infringement of copyright in digital platform are as follows:

1. In case of conducting research and caring out teaching related work based on material available on internet
2. Access to online database like e-books and journal on University website or library
3. Making and adopting of computer program for personal use and for commercial use
4. Publication of speech delivered in public
5. Reproduction of any electronic reports, policies, of any committee, council, institutions established by the Act of the legislature or by State and Central Government, etc.

Remedies for Infringement of Copyright on Digital Platform

Online Piracy has become rampant in digital era. This has posed a greater challenge to the copyright owners and creators. Due to insufficient guidelines and lack of remedy, the rights of the owners are getting affected. Even though there are different remedies available under the Copyright Act like Civil, Criminal and Administrative, but due to changing scenario and dependence on technology paves new kind problems which in turn is very much challenging even to the judiciary to handle the situations. Let us look at recent cases where judiciary played vital role in balancing the situation. However Hon'ble Delhi High Court in

[13] Nehal Wagle, Copyright in Digital Era, https://blog.ipleaders.in/copyright-digital- accessed 28th March 2021
[14] Ibid
[15] Supra note 10

its recent judgment dated 10th April 2019 in case of UTV Software Communication Ltd & Ors. vs. 1337X.TO & Ors.,[16] has provided for sufficient remedy with the concept of Dynamic Injunction.

UTV Software Communication Ltd & Ors. vs 1337X TO & Ors.

In the present case the plaintiffs had a several companies engaged in the business of creating, producing and distribution of cinematographic films across the Globe including in India.[17] The plaintiff filed eight suits against defendants seeking injunction, restraining the infringement of copyright by communicating to public the plaintiff's original content/cinematographic works without authorization.

Issues Raised Before the Court:

1. **Whether an infringer of copyright in physical world is treated to be different form infringer on internet.**

Answering the issue in negative, the Hon'ble Court observed that there is no logical behind why the crime in the physical world is not a crime on digital world, as there is no such distinction made under Copyright Act.

2. **Whether seeking blocking of a website dedicated to piracy makes one an opponent of free and open internet?**

Answering the issue in negative, the Hon'ble Court made an observation that the key issue about the freedom to use internet. Here the question is whether internet should be completely free or the Government should have given unlimited censorship authority, rather where to draw appropriate lines, how it should drawn and how it has to be implemented, all these factors need to be focused.

3. **What is 'Rogue Website'?**

These are such a websites which are primarily meant for sharing the infringing/ pirated content to the public. They themselves allow streaming of the content and provide searchable database with the link to the third party. These websites invite the people I mean

[16] CS (Comm) 724/2017
[17] Rajat Sabu, "Remedies against Online Piracy to Protect the Internet of Copyright Owners: A New Approach by way of Dynamic Injunction", https://www.khuranaandkhurana.com/2020/04/22/r, accessed April 22nd 2021

public for watching free movies/contents. Some of these websites provide entire module/interface, so that the users are allowed to watch pirated content/ movies by way of links.

The Hon'ble Court in the present case clarified that the aforementioned factors are illustrative and not exhaustive & it doesn't apply to intermediaries as they are governed by IT Act, having the statutory immunity.

4. **The test for determining a 'Rogue Website' should be qualitative or quantitative?**

The Hon'ble court was of the opinion that to declare the test as rogue website, it should contain only illicit or infringing content or material, but in case if each and every rogue website add small content or percentage of legitimate material and it will pray to be declared not an infringing website. Then, it is appropriate to apply a qualitative approach and not a quantitative, in case of real test for examination of Rogue Website.

5. **Whether the website of the defendant fall with in the category of Rogue-Website?**

As per the observation of the court, it is very much clear that there is sufficient proof or evidence on record to prove that the defendant's websites are committing or facilitating for copyright infringement by providing the access to a large library of films, including films of the plaintiff without taking authorization. In addition to this there is one more issue fall within this preview,

6. **Whether the court would be justified to pass the directions to block the 'Rogue Website' in entirety?**

The Hon'ble court made very keen observation that the blocking of the rogue website needs to be handled carefully and at the same time it has to strike the balance between the preserving the benefits of free and open access to internet and the efforts are needed to stop the crimes that are happing on digital platforms, called as digital piracy.

The most significant role played by the court in the present case is by creating the new way or procedure, to extend the support for website blocking injunctions beyond the websites specified in the order and this kind of injunction is called as **'Dynamic Injunction'** which shall extent to the websites which are redirect websites that have created subsequent to the

injunction orders.[18] The court made it clear that this Dynamic Injunction order is stemmed from the decision given by Singapore Court. Further the court made it clear that awarding such kind of injunctions will fall in the power of the court under Section 151 of Civil Procedure Code.

Shamoil Ahmad Khan vs. Falguni Shah and Ors.[19]

In the present case plaintiff is the author of popular short story **'Singardann'**. The defendant is the producer and started web series with the same title and story of the plaintiff. Plaintiff became aware of defendant's web series and then he approached the court seeking injunction against the defendant. Both of them had same based script.

The court after reviewing the facts and evidence produced before it, it was decided that the there would be violation of copyright if similarities are based on substantial aspects of the mode of expression adopted in the copyright work. In the present case the court found a substantial similarity in both the storylines and ordered the defendant to stop from making further adaptation or use of web series by name of **'Singardaan'**. Matter is pending for final disposal of the suit.

Vinay Vats vs Fox Star Studios India Pvt. Ltd and Ors[20]

The plaintiff was a writer and defendant was production house. Plaintiff own the copyright for his original script on which they have come out with the film titled **'TukkaaFitt'** . The allegation of plaintiff against the defendant is that the film **'Lootcase'** produced by defendant, has same story as the film **'TukkaaFitt'**, produced by M/s. AAP Entertainment Limited. The plaintiff filed the law suit against the defendant by claiming that the film **Lootcase** was recently brought to his attention and when he watched the trailer, the Plaintiff noticed several similarities between both the movies.

The court observed that, in case of copyright related work the protection under the Act can be given for expression of an idea and not idea itself, this expression of idea can be done in several ways. In this case court made clear statement that in order to determine two films are exactly same we need to be relied up on the audience's reaction about both the movies.

Anyway with this note court come to the opinion that the balance of convenience lay in favor of the defendant. The court was not convinced by the claims put forth by the plaintiff. The

[18] Supra note 12
[19] MANU/MH/0590/2020
[20] CS(Comm) 291/2020

matter got decided in favour of defendant and dismissed the plaintiff's plea for grant of an interim injunction.

Jagran Prakashan Limited vs. Telegram FZ LLC & Ors[21]

The plaintiff owed a publishing company and published leading newspapers in Hindi, popularly known by name **'Dainik Jagran'** and he also registered under Trade Mark Act couple of marks as associated trademarks for his newspapers. The reader has an option either to subscribe for physical or can have it online, I mean digital version of newspaper form corresponding webpage. The subscriber on digital platform could only access newspaper but can't download the PDF version. The defendant come up with cloud based instant messaging service called Telegram and the app version of this service is available on several operating systems for users to download. This helped the users to anonymously start various channels and post the content on these channels. Plaintiff sent several notices to defendant and requested to shutdown the infringing channels but there was not response form defendant side, then plaintiff filed lawsuit in Delhi High Court.

After examining the evidence produced by the plaintiff, the court favored the plaintiff and granted an ad-interim injunction. Further the court agreed with the contention of the plaintiff, that the defendant could not continue to claim the intermediary status and at the same time the court ordered the defendant to block the infringing channels and to disclose the names of all the users who started the each of these channels.

Conclusion and Suggestions

Considering the above discussion, it is very much clear that digital era provided ample opportunities to the creative minds, I mean to the creators to come up with their work and creations in an effective way, but on the other way round it has raised the greater concerns for infringement of the rights belonging to owners or creators. However, the lot of efforts has been made by the implementing new laws and at the same time amending the existing laws and in addition to this, the judiciary also played the significant role to overcome the obstacles and to ensure the protection of the rights of the copyright holders in the digital platform, but still, we can find a lacuna and which need to be addressed with proper measures.

There are certain things one must keep in mind while using your work on digital platforms:

[21] CS(Comm) 146/2020

- Proper training and creating awareness to the public on the usage of digital platform needs to be focused
- Copyright issues have to be addressed by proper application of the Doctrine of Fair Use.
- Training has to be done for enforcement agencies.
- To develop a proper mechanism to prevent copyright infringement by adopting the best practices of other countries.
- The new preventive techniques like Blockchain technology, Digital Watermarks, and other kinds of software have been used to control the infringement on the digital platforms. All these techniques need to be explored in order to ascertain how far they are useful in handling the problems on digital platform.

IMPACT OF TECHNOLOGY ON LEGAL PROFESSION AND EDUCATION IN INDIA: AN OVERVIEW

Dr. Dnyaneshwar P. Chouri[1]

ABSTRACT

Technology has revolutionized the way, ease, speed and time with which we conduct our activities. Business transactions are conducted faster, learning and teaching are richer, and generally the legal profession is better positioned. The legal profession is known for its conservatism and traditionalism which many believe must be preserved in order to maintain the prestige of the profession. However the wave of technological advancement and globalization which has swept through various aspects of the society has not left the profession in its path. The technological innovations are influencing the legal education and practice of law. Consequently, lawyers and law students will need to develop new skill sets in order to thrive professionally.

Though there are huge benefits conferred by the use of technology in legal education and practice, there are some challenges for effective utilization of technology in the legal profession and education is the lack of internet or technology culture among law teachers and their students on the one hand and lawyers and their clients on the other hand. While many advanced jurisdictions have been able to inculcate the technology/internet culture, Many law teachers, students and lawyers are still in the analogue and paper world; unwilling to change or adapt to the sweeping technology culture. This could be due to sheer conservatism or a general distrust for the internet and technology. This paper will mainly focus on emerging impact of technology on legal profession & education. The paper also examines emerging challenges in effective utilization of technology in legal profession and education and way forward in advancing techno-legal development in India.

❖ LEGAL PROFESSION

Information Communication Technology (ICT) is an umbrella term that includes all technologies for the manipulation and communication of information. The work of legal practitioners involves a high level of documentation and information processing, storage, and retrieval. The information intensiveness of a lawyer's responsibility is such that tools and technologies that would speed up the documentation, management and information handling

[1] Assistant Professor, KLE Society's G. K. Law College, Hubballi, Karnataka

are not only important but professionally necessary. The value of accuracy, correctness, completeness, relevance and timeliness are characteristics of information which ICT systems do generate to meet lawyer's information needs. The role of lawyers in any society is essential, especially in defending his client (s) in the court of law by applying the principles of law to the evidence available, by providing relevant facts. Lawyers enlighten the public of their constitutional rights and ensure that people are not deprived of their fundamental human rights such as freedom of association, speech, opinion, religion etc.[2] The impact of technology on legal practice has been monumental, with the progressive automatisation of tasks and increasingly fluid cross-jurisdictional working. Automatisation has led to an undeniable evolution in the role of legal professionals, and whilst the pessimist among us suggests this limits the scope of individuals' work, the optimist perceives more refined and critical work for the lawyer, who is able to focus on the most demanding aspects of legal practice, leaving more mundane tasks to machines.[3]

Legal Professionals and Required Skills

In legal practice it is expected that the legal professionals to maintain certain standards of professional competence and ethical behavior. Throughout their careers it is required of lawyers to ensure that they keep updates regarding the law in their practice area and maintain the knowledge and skill necessary to fulfill their professional responsibilities. These skills may include business management, enhanced firm operation and procedure, practice management and quality control of services, client relationship management and development, product analysis and development, marketing of services etc. If lawyers could be equipped with these skills early in their careers they would develop into legal professionals who could, for example, be charged out to clients at a higher rate.

[4]

- **Employment of technology in Legal profession and Legal Research**

Since the law is a profession and professionals have an assumed expertise in a specific body of knowledge, lawyers are considered as knowledge workers. Knowledge workers are defined by their relationship with information. Lawyers as knowledge workers adhere to a

2 Jide Owoeye, Information Communication Technology (ICT) Use as a Predictor of Lawyers' Productivity @ Library Philosophy and Practice (e-journal) | Libraries at University of Nebraska-Lincoln | University of Nebraska - Lincoln (unl.edu)

3 Technology: Implications on the Nature of Legal Practice and the Role of the International Legal Profession, Available @ https://www.sheffield.ac.uk/media/951/download.

[4] T du Plessis, Competitive Legal Professionals' Use Of Technology In Legal Practice And Legal Research, Per 2008(4), PP.38-39

minimum standard of professional competence and the premise is that lawyers have a professional responsibility to research and know the law to serve in a client's or the public's best interest. A lawyer's duty to research and know the law has a strong ethical component. Equally important is the application of malpractice standards not only to traditional legal research, but also to electronic research. For example, the Internet currently provides access to information resources that previously would not have been readily available, and this requires modern lawyers to possess a high level of electronic research skills to find, amass, manage, evaluate and use all readily available, relevant and authentic information to serve a client's case or matter. In the information era lawyers cannot claim to be knowledge workers without effectively using the ICTs, the Internet and other electronic resources for legal research if the situation so requires.[5]

One of the biggest steps that have enabled technology in law to involve is the digitalization and storage of case law, statutes, and regulations. Recently, Harvard Law School has made their entire Collection of case law available to the public. This has enabled technology firms to aggregate, store, and provides statistics about the law in a way that we have not seen in the past. Artificial intelligence is on the rise and may change how legal research is done. Recently, the company called ROSS Intelligence has started using the IBM computer called Watson in order to perform legal research. Specifically, they are attempting to get Watson to understand and interpret the legal terminology used by lawyers in order to look up case law and statutes. Other firms are developing similar technology that will enable lawyers to delegate the task of reviewing contracts to a computer. Some firms are even trying to develop intelligent contracts that can alter themselves based on a variable set of information.[6]

- **Impact and Challenges of Technology in Legal Profession**

Perhaps the greatest obstacle to the introduction of ICT into any program relates to resourcing. Development usually requires the necessary software, the programming and design expertise and the time to create materials.[7] The legal impact of technology suggests

[5] *Ibid*, P.40
[6] Bruce Burk, New Technology and Its Impact on the Practice of Law, Available @https://www.expertinstitute.com.
[7] Butler, D. (2007) ICT in legal education: a challenge but an opportunity, in Enhancing Higher Education, Theory and Scholarship, Proceedings of the 30th HERDSA Annual Conference, Adelaide, 8-11 July 2007: Published 2007 by the Higher Education Research and Development Society of Australasia, Inc PO Box 27, Milperra, NSW 2214, Australia, p.12

that focus should be on how the current information revolution is affecting the tenets of the law. In addition to transforming the approach of experts to legal information, e.g. the development of fields such as artificial intelligence (AI) and the law, technology has brought on new types of lawsuits, or modified existing ones. Consider new offences such as computer crimes (e.g. identity theft) that would be unconceivable once deprived of the technology upon which they depend. In accordance with the clause of criminal immunity summed up, in continental Europe, with the formula of the principle of legality, i.e. "no crime, nor punishment without a criminal law" (nullum crimen nulla poena sine lege), this is why international lawmakers decided to intervene with the Budapest Convention on Cybercrime in November 2001. Moreover, reflect on traditional rights such as copyright and privacy, both turned into a matter of access to, and control and protection over, information in digital environments. By examining the legal challenges of technology, we thus have to specify those concepts and principles of legal reasoning that are at stake. Then can we begin to determine whether the information revolution: (a) affects such concepts and principles; (b) creates new principles and concepts; or, (c) does not concern them at all, the latter being the view of traditional legal scholars.[8]

AI has currently presented the deepest and most profound impact on law, legal practice and legal education. The impact of AI is far more than improving efficiency and productivity: AI has the potential to replace lawyers in many of the traditional areas of practice, and indeed, it is generally agreed that AI can be more accurate and efficient in tasks demanding high technical skills. As such, the advancement of AI technologies and their application can be seen as threatening jobs and opportunities. This is especially so if AI is examined from a developing perspective: at the moment, it is generally agreed that AI would replace low-level skills, thus impacting on paralegal and junior lawyer jobs. But in the longer term, it is also agreed that AI could replace some high-level skilled roles currently performed by lawyers.[9]

Legal practice is not all about technical matters and skills; it is fundamentally about achieving justice and fairness through not only interpreting and applying the law, but also by

[8] New Technologies And Law: Global Insights On The Legal Impacts Of Technology, Law As Meta-Technology And Techno Regulation, https://lawschoolsgloballeague.com/wp-content/uploads/2017/01/New-Technologies-and-Law-Research-Group-Paper-2015.pdf

[9] Zhiqiong June Wang, Western Sydney University, Between Constancy and Change: Legal Practice and Legal Education in the Age of Technology, Vol 36 No 1 (2019): Law & Society and Law & Technology, Available @ https://journals.latrobe.edu.au/index.php/law-in-context/article/view/87/165

advancing the law with empathy, compassion, and a strong sense of justice and ethics. Lawyers need to be masters, not servants, of technology. Even in interpreting and applying the law, technical skills and rules the underlying mechanisms for AI technologies in law are in fact rules laid down by human beings. These technologies and mechanisms create their own risks and limitations, and understanding these risks and limitations is critical for legal practice.

❖ THE LEGAL EDUCATION

Higher education is inescapably subject to technological forces, both in the context of new modes of delivery as well as substantive knowledge and disciplinary insights informed by technological progress.[10] The legal education sector prepares the judges, practitioners and scholars of tomorrow. The quality of justice delivery in the future is dependent on the training and exposure that we are able to provide to present students. Hence, it is important to continuously assess the challenges faced in the delivery of legal education. The present study can be treated as another effort in this direction. The distinctive feature of this particular study is that it has been conducted with the explicit intention of generating actionable recommendations. An instrumental approach will be visible in this report and some readers may find that our discussion foregrounds practical considerations over conceptual analysis.[11] The provision of high quality legal education is a pre requisite to high quality legal practitioners, judges and Government law officers. The need for such education is felt not only in the developing and underdeveloped countries but also in the developed nations who have deemed it necessary to assess and revise curricula and methodologies of law courses with an objective to update them for meeting new challenges and needs of their societies.[12]

Law Teachers and Required Skills

"If a teacher today is not technologically literate - and is unwilling to make the effort to learn more - it's equivalent to a teacher 30 years ago who didn't know how to read and

[10] Allan Collins and Richard Halverson, Rethinking Education in the Age of Technology: The Digital Revolution and Schooling in America (Teachers College Press, 2nd ed, 2018); Andreas M Kaplan and Michael Haenlein, 'Higher Education and the Digital Revolution: About MOOCs, SPOCs, Social Media, and the Cookie Monster' (2016) 59(4) Business Horizons 441.

[11] A Study To Create Evidence-Based Proposals For Reform Of Legal Education In India - Suggestions For Reforms At The National Law Universities Set-Up Through State Legislations (Draft of Final Report), Implementing Organisation: NALSAR University of Law Justice City, Shameerpet, Hyderabad, Medchal District, pp.108

[12] Mayank Shekhar, Challenges Of Legal Education In The 21st Century, Available @ https://www.legalbites.in/challenges-legal-education-21st-century/

write ."[13] Innovations in teaching have the potential to provide and liberate, but there exists also a responsibility on lecturers to ensure they do not prevent and restrict access to learning. The increasing pervasiveness of ICT into the realm of the law teacher or lecturer offers an opportunity for increased engagement with a wider variety of learners. In some instances the characteristics of these users are known and can be directly catered for, but in some cases the user audience (or at least their specific requirements) are not known. The range of possible characteristics and needs across this audience is potentially as large as within the general populace, and online resources must be designed and created with this factor very much in mind. However, this does not mean that creativity need be limited, or that materials that are inaccessible to some cannot be used to bring benefits to others.[14]

Every new technological development in teaching history has received some sort of pedagogical criticism, often based on an initial fear of a replacement of the teacher, as well as a general lack of knowledge and/or familiarity regarding the new technology. However, most of those feared detrimental effects never materialized. Indeed, those concerns often were forgotten or the new technology was absorbed into teaching in various forms. With respect to computer display technology in the classroom, because history is again likely to repeat itself, display technology should not be feared as a modern replacement of the teacher, but instead should be accepted as a natural step in the inevitable evolution of classroom teaching.[15]

The technology helps the law teacher in many ways like the kinds of skills that can most effectively be taught online; personnel requirements for developing and offering online courses; the pros and cons of asynchronous online formats; differing online social norms of behavior; optimum class size for online delivery; access and administration issues etc.[16] Teachers can use course management sites like TWEN and Blackboard to share information and manage basic course functions. Despite these profound changes, legal education has never considered technological proficiency to be a key outcome. Law professors may debate the merits of audiovisual teaching tools. Many fear that laptops and other devices distract students in class, and some institute outright bans. Among many law professors, technology

[13] Fisch, 2007, winner 'Most Influential Blog Post, EduBlog Awards 2007.
[14] Simon Ball, Making Law Teaching Accessible and Inclusive, Electronic Law Journals Journal of Information Law & Technology, JILT 2009 (3) – Ball, Available@ https://warwick.ac.uk/fac/soc/law/elj/jilt/2009_3/ball.
[15] By Fred Galves, Will Video Kill the Radio Star? Visual Learning and the Use of Display Technology in the Law School Classroom. Available @ https://law.bepress.com/cgi/viewcontent. Pp.5
[16] Jacqueline D. Lipton, Distance Legal Education: Lessons From The *Virtual* Classroom, Available @ https://poseidon01.ssrn.com. P.1

is warily accepted, but only for the purpose of achieving traditional educational objectives. If educators viewed technology as a competency that teachers and students needs to master in order to succeed in practice it will change the ways what we teach, and the way we teach, to address the disparity; considers the benefits and drawbacks of developing new courses, or infusing technology-related outcomes throughout the curriculum; and proposes methods to encourage professors to teach with technology in ways that model the practices of successful attorneys.[17]

Employment of Technology in Legal Education and Legal Research

Computers have a very important role to play in the modern legal education and research. For instance, law schools have to generate a variety of written materials for students as well as for other academic purposes, such as, for conferences, meetings, moot-courts, seminars and workshops. Almost every law faculty has to supply to the students, the summaries of case law which are normally printed every year by the university press and the cost of printing is sometimes enormous. Every time the faculty has to pay the printing and composing charges a fresh. However, if the text is once typed and stored in the memory of a computer, the required materials can be printed out any time. This is likely to be relatively much less time consuming as well as much less expensive exercise in comparison to the printing business. With the computer facilities available in a law school or a law faculty, all other types of expenses, say for example, expenses on cyclostyling can also be saved. Once we have a master print of the required document, it can be easily photocopied and distributed amongst the students. Similarly, students can also type and prepare their project reports and other academic assignments on computer, provided the facility is available to them, too. Nowadays, computers are also being considered as valuable aids in the law teaching. As a matter of fact, there are so many ways in which computers can be of a great help and utility in the modern legal education." Computers have an equally significant role to play in legal research. For instance, every researcher working for a post-graduate essay, an M.Phil. or an LL.M. dissertation, or for a Ph.D. thesis has to prepare a working bibliography. In the normal practice, researcher writes down the names of the references and bibliographical sources on plain pages or on reference cards. Later on at the time offinal report writing, the researcher has to arrange those cards in bibliographical order and hand it over to the typist. If a single card is wrongly arranged, it is likely to be wrongly typed. Moreover, if a researcher is

[17] Simon Canick, Infusing Technology Skills Into The Law School Curriculum, Available @ https://core.ac.uk/download/pdf/56360844.pdf, PP.1-2

engaged in research on a topic on which literature appears quite frequently in journals, articles and newspapers etc., researcher may have to update the text from time to time and very obviously the entries in the bibliography shall also change. The major problem arises when the dissertation or the thesis is at the typing stage and some significant case is decided by the higher judiciary or some relevant literature appears which a researcher finds absolutely important to incorporate in his study. If the researcher is working on a computer, s/he need not prepare any bibliographic cards. Once bibliographical entries are put into computer's memory, they stay there forever. One can add, remove or make any type of modification in them without re-writing anything. In case, any entry needs to be dropped at the last moment, one can remove them easily. Similarly, if any entry in case list or even in the text of the dissertation / thesis is to be made at the last stage, it can be made without any hassle. In this process, the computer will automatically adjust the new entry and the page sequence shall not be disturbed at all. Another great advantage of data processing through computers is that a researcher can make use of bibliographical sources even after she/he has submitted the dissertation/thesis etc. If she/he wants to list some of the references for some article or research paper there is no need for re-typing them at all. The required references can be selected and very easily copied on another computer file opened by the researcher and the original bibliography stays there without any modification whatsoever. The same is applicable to the entries in the list of cases, list of statutes and glossary of acronyms and abbreviations and even to the chapters. One of the important benefits of computer-assisted legal research is that the text of anything typed in the computer can be stored there forever. It can be changed, modified and/or remodified by the researcher up until even the last day before the text is finally printed. Very obviously there does not arise any need for re-writing of the entire text. Moreover, if some paragraph is to be omitted and another paragraph is to be inserted, there is no need to write the entire page. The computer adjusts this change automatically.[18]

Challenges posed during Covid-19

Of course, the privileged class of society and institutions within a few days of national lockdown suddenly responded to the calamity positively by organizing and circulating links to “webinars” being hosted on various legal topics, various workshops on legal education, national and international seminars through webinars what not even the online internship

[18] Gurjeet Singh, Role Of Computers In The Fields Of Legal Education And Research, Available @ http://14.139.60.114:8080/jspui/bitstream

programmes were offered by legal firms. The pandemic situation highlights some of the unfortunate reality of legal education. In spite of lack of proper infrastructure, many legal educational institutions forced its faculty members to take the online lectures to complete the syllabus. No doubt, the National Law Schools in our country and other private law schools with good infrastructure who already provides laptop and other facilities might not have burdened with this new phase of teaching. However, there are many institutions, though recognized by the Bar Council of India (BCI), where majority of not so privileged students with bright legal acumen are studying and aspiring to be part of bar and bench. They might have faced a huge problem to access the online classes or may be cannot afford the cost of technology.[19] The platform used for online teaching posed challenges because of lack of institutionalized platform to impart the lectures. Those who were technically savvy used this opportunity and became the masters of online teaching without analyzing the impact of the same.

Impact and Challenges of Technology in Legal Education

Despite the huge benefits conferred by the use of technology in legal education and practice, there are some challenges that make the effective utilization of technology in the legal profession. The first challenge is the lack of internet or technology culture among law teachers and their students on the one hand and lawyers and their clients on the other hand. Many law teachers, students and lawyers are still in the analogue and paper world; unwilling to change or adapt to the sweeping technology culture. This could be due to sheer conservatism or a general distrust for the internet and technology. The situation has however changed and no one can stop the wave of technology sweeping over the world at the moment. The current law students were introduced to computers and the internet at a much younger age than their teachers. An internet/web culture therefore needs to be cultivated by lawyers, law teachers and students.

The high cost of technology may also be responsible for the low response to it. Not only do computers and other ICT devices or hardware need to be purchased but a constant upgrade and maintenance will also be required from time to time. Majority of the law firms are however sole proprietorships which cannot afford such capital intensive investment. The

[19] Susmitha P. Mallaya, Contouring Legal Education In India: An Analysis Of Challenges Posed By Covid-19, ILI Law Review, Special Issue 2020, P.148

same problem also applies to law faculties since there are no sufficient funds allocated by the government for the education sector.

Most law faculties within the country do not have adequate computers, projectors or internet connectivity within the classroom. In addition, quality online legal research is not usually free. Money is required to subscribe to sites such as Westlaw, LexisNexis Manupatra etc. Academic journals also require subscription fees whether individual or institutional which many law faculties and firms cannot afford. The non-availability of fast high speed internet also adversely affects the use of ICT in legal education, research and practice. Some mobile networks are also unavailable or not good in certain locations. The high cost of internet service must also be taken into consideration. All these impede the influence technology has in the legal profession. Furthermore, almost all technological devices require electricity to work effectively.

A major challenge to the law teachers contend with in the use of internet by law students is that of plagiarism. The internet and technology makes it easy for students to plagiarize the works of others by simply copying and pasting information found on the internet as theirs. The situation could be worse where students collect the soft copies of someone's thesis and merely effect a change of personal information and institution while presenting same as their own research work. The fact that technology and internet makes plagiarism easier is uncontestable. One of the consequences of the impact of the technology/internet is the availability of many legal templates online at little or no costs to potential or actual clients.

Apart from this, there is a strong movement to digitalise education sector as well with the objective of promoting digital India movement. This will promote online mode of education along with the traditional mode of teaching. UGC framed and notified the regulations in this regard to recognise and streamline the granting of online degrees at the undergraduate and post graduate levels. It lays down the minimum standards of instruction for the grant of degrees of post graduate diploma, through open and distance learning mode and online mode.[20] It encourages self-learning mode through online platform like MOOCS, SWAYAM which will enable the learner to learn through e-module which is inter alia self-

[20] University Grants Commission (Open and Distance Learning Programmes and Online Programmes) Regulations,
2020, Sept. 04, 2020, available at: https://www.ugc.ac.in/pdfnews/221580.pdf .

explanatory, self- contained, self-directed at the learner, and amenable to self-evaluation, and enables the learner to acquire the prescribed level of learning in a course of study and includes contents in the form of a combination of the following e-learning content like e-text materials, video lectures, audio-visual interactive material, virtual classroom sessions, audio pod casts, virtual simulation and self-assessment quizzes or tests. This approach from the part of UGC shows the need to implement certain measures in tune with the same in the field of legal education as well and there is a need for BCI to prepare a roadmap and discuss the same with all stakeholders of legal sector.[21]

Conclusion

Machine is fast replacing human efforts in the provision of certain legal services particularly with the employment of Artificial Intelligence (AI) technology. The implication of this is that lawyers will be getting lesser jobs, especially when it comes to agreements and procedures such as e-discovery. To have machines replace lawyer's work would make the situation worse. Therefore, it is apparent that it is time for lawyers to begin to carve a niche for themselves in order not to lose out. Lawyers must begin to focus on areas of 'lawyering' where they are indispensable and are irreplaceable by machines. A successful legal practice in the nearest future will be that which adjusted itself to changes in technological advances including AI as well as delivers the parts of legal services which machines cannot provide. Machines and quacks can definitely not replace lawyer's service because even in drafting legal documents, the client does not only get a valid document but also some level of guarantee that such a document will be able to achieve the desired result due to the lawyer's competence and experience. Similarly, though empirical testing of the impact of technology in legal education has not been undertaken, the cornerstone of legal education is technology. What is expected from legal education is not only to create philosophers and jurists but also to mould a smart technical craftsman who is able to take a broad view of the functions of law and realise their duty to society as lawyers.

[21] *Supra* note 18, P.154.

E-COURTS: START, PANDEMIC RESPONSE AND FUTURE

Keshav Bansal[1]

ABSTRACT

"This research aims to unfurl the development of e-courts in India and what the other countries are doing. The study analyses the e-court mission mode project and the pandemic response. An empirical method of approach combined with theoretical analysis has been taken for the research. The scope of research is limited to identifying lacunae in the existing system and does not deal with the solution. The analysis is that the judiciary was not prepared for the pandemic despite the e-courts project being started in 2005.The study results in the conclusion that judiciary needs to separate the administration from the judicial function to implement technological solutions effectively."

INTRODUCTION

Access to justice is one of the challenges that judiciary has always faced. With the advent of internet technologies, things started to change but where changing slowly. The pandemic has forced the judiciary in order to keep its door open, it has to scale up its Information Technology (IT) infrastructure. Now, courts have to invest more than ever in infrastructure of IT. This is need of the hour but while expediting the process legal principles and data principles need to be kept in mind and should move forward with caution. AD-hoc measures that have been taken may not be the best solutions and there is a need for reassessment of the same. We need to look back towards the Online dispute resolution (ODR) platforms already in existence and work towards assimilating it with e-courts.

When the dawn of internet came upon India, the judiciary started the E-courts project 20 years ago to lay down the required technological infrastructure. The pandemic is the time to build upon the groundwork for accelerated integration of judiciary with technology. Generally putting forth, the pendency of cases has expanded altogether at each level of the legal pecking order in the most recent decade. Among 2006 and now, there has been a general increment of 22% (64 lakh cases) in the pendency of cases across all courts. As of August 2019, there are over 3.5 crore cases forthcoming across the Supreme Court, the High

[1] First Year Student GNLU

Courts, and the subordinate courts. Though recently the strength of the Supreme Court has been increased but the ratio of judges to cases and increasing efficiency in that manner is outside the scope of this research.

E-courts are well suited for the country with the exponential rise in internet users. With a surge in internet users (who constituted 34.8% of the population or 462 million people in 2016), the idea of virtual courts is more viable now than ever before.[2] Integration of technology has fastened, and justice delivery system is being expediated. It is not with caution that the principle of open justice should not be violated.

ODR TO E-COURTS

ODR mechanism is for resolving disputes facilitated through the use of electronic communications and other information and communication technology.[3] As globalization took place, companies across borders started having contracts with each other. With this was recognized a need to have a platform to redress the dispute without incurring heavy expenses. As the disputes were cross border, the Jurisdiction was an issue, ODR took way. E-bay and square trade started the first ODR platform in 1999.

Alternative dispute resolution (ADR) was integrated into ODR first as an alternative to judiciary as it had its limitations. ODR saw an explosion in its use due to advent of e-commerce websites. But there are some differences between ODR and e-courts which needs to be duly noted.

ADR in a virtual setting is done by the mutual consent of both the parties and is restricted to civil cases whereas e-courts will have physical evidences, cross examination and criminal cases. E-courts may be applicable to all the parties and may not partake their willingness to be part of online proceedings. Judicial Process is one which has sanctity by way of law, and violation of privacy can't be afforded.

ODR today exists in three ways: 1. Private ODR with ADR 2. Court annexed ADR 3. E-courts. The third way is the focus of this paper.

[2] Vidhi legal Policy, Virtual courts in India: A strategy paper accessed on 03 January 2020

[3] United Nations Commission on International Trade Law, 'UNCITRAL Technical Notes on Online Dispute Resolution, <http://www.uncitral.org/pdf/english/texts/odr/V1700382_English_Technical_Notes_on_ODR.pdf> accessed 02 January 2020

E-filling, E-notice through mediums such as e-mail, SMS, Whatsapp etc., Virtual hearings, Documents' exchange, Identity and access management, Storage and retrieval of digital data, Payment integration, Private break-out rooms for decision makers / parties, Smart Scheduling Digital Signatures are some of the common features between e-courts and ODR platforms.

Though immediate needs are being fulfilled by existing video conferencing solutions, sooner than later the court needs to develop its own platform due to various security reasons.[4]

E-COURTS: WHERE ARE OTHER COUNTRIES?

In United Kingdom (UK), Her Majesty's Courts and Tribunals Service (HMTCS) document, governs the virtual courts and provides some guidelines.[5] Also the Coronavirus Act, 2020 provides for virtual hearing with compliance of the Open justice principle.[6]

In United States of America (USA), various states have their own laws regarding virtual hearings. In general, ODR principles and guidelines, Uniform Domain Name Dispute Resolution Policy[7], ODR standard of practice by national centre for centre and dispute are being followed.[8] New York is having hearings virtually for matters that are not essential too in the pandemic.[9]

In China 3 cities, Hangzhou, Beijing and Guangzhou have started e-courts back in 2018. In these places, from filing to judgement, the whole process is virtual. Also 'we-chat' is being used for resolution. Cases have started in online mode for the pandemic as was decided

[4] Aditya AK, 'Home Ministry division issues guidelines for safe use of Zoom amidst security concerns' (Bar and Bench, 16 April 2020) <https://www.barandbench.com/news/home-ministry-division-issues-guidelines-for-safe-use-of-zoom-amidst-security-concerns> accessed 03 January 2021

[5] HM Courts & Tribunals Service, Guidance: The HMCTS Reform Programme (2019) <https://www.gov.uk/guidance/the-hmcts-reform-programme> accessed 03 January 2021.

[6] Coronavirus Act 2020, Schedule 23-25 <http://www.legislation.gov.uk/ukpga/2020/7/contents/enacted> accessed 03 January 2021.

[7] ICANN, 'Uniform Domain-Name Dispute-Resolution Policy' <https://www.icann.org/resources/pages/help/dndr/udrp-en> accessed 04 January 2021.

[8] Advisory Committee, National Centre for Technology and Dispute, 'Online Dispute Resolution Standards of Practice' <https://www.icann.org/en/system/files/files/odr-standards-of-practice-en.pdf>. accessed 03 January 2021

[9] New York State: Unified Court System, 'Press Release: Virtual Courts Expanded Beyond the Limited Category of Essential and Emergency Matters' (13 April 2020) <https://www.nycourts.gov/LegacyPDFS/press/PDFs/PR20_15virtualcourtstortsetc.pdf> accessed 04 January 2021

by the Chinese Supreme Court.[10] China has a small court framework which enhances the public trust in judiciary. It also has the largest repository of cases online.

E-COURTS: THE INDIAN DREAM

The e-courts mission mode project started in 2005 when Supreme court made a E-committee. This project ambitioned to integrate ICT in all the district courts of the country.[11] This project has been able to provide a lot of services for litigant as they can, the case status, electronic cause lists and have access to them in pdf format. National judicial data grid has been one of the best things about the project.[12] The NJDG is a data gathering portal which tracks pending and disposed cases across all the High Courts, District and Taluka Courts in India, in real time, and has emerged as a significant tool for empirical data collection on court performance.

Phase 1 of the project wanted to lay down the requisite infrastructure such as internet, hardware and software for courts to make virtual hearings possible. The e-courts project uses open source software which is in compliance with open data principle. Additionally, it is also cost effective. Some applications are also being launched for e-payment and e-filing.[13] Now, virtual courts are being set up to resolve traffic challan related offences.[14]

Though the infrastructure may be there, there has not been adoption of the system. Around 2 lakh cases were instituted in 2019 out of which not even 1000 were filed online.[15] It is because the interface is not user friendly, and the lawyers are not trained how to use these systems.

[10] The Supreme People's Court of People's Republic of China, 'Chinese Courts, Internet Judiciary in Data' (18 December 2019) <http://english.court.gov.cn/2020-02/13/content_37533572.htm> accessed 04 January 2021.
[11] E-Committee, Supreme Court of India, National Policy and Action Plan for Implementation of Information and Communication Technology in the Indian Judiciary (2005) <https://main.sci.gov.in/pdf/ecommittee/action-plan-ecourt.pdf> accessed 04 January 2021.
[12] Supreme court of India, National Judicial Data Grid, <https://njdg.ecourts.gov.in/hcnjdg_public/index.php> accessed 04 January 2021.
[13] Press Information Bureau, 'CJI Launches Applications to Facilitate Litigants and Lawyers' (23 August, 2018) <https://pib.gov.in/newsite/PrintRelease.aspx?relid=182015> accessed 17 April 2020,; E-Committee Supreme Court of India, User Manual National Service and Tracking of Electronic Processes <https://ecourts.gov.in/ecourts_home/static/manuals/NSTEP-User%20manual.pdf> accessed 04 January 2021
[14] NIC eCourts Services Transforming Judiciary for Effective Justice Delivery (n 52) 24
[15] eCourts India, Innovations: Phase II eCourts Project, 33 <https://ecourts.gov.in/ecourts_home/static/manuals/FINAL%20INNOVATIONS%20IN%20PHASE%20II.pdf> accessed 28 April 2020

The phase 1 of the project aimed to be completed in two years, took eights to see light of the day. This shows the lack of co-ordination between different stakeholders and unrealisable timelines being set. Under-utilisation of funds is a major problem, In phase II approved in 2015, the budget approved was of 1670 cr. But only 700 cr. Have been utilised.[16] The concentration of administrative and judicial functions in the judicial officers has been a root-cause for inefficiencies on the administrative side, which eventually manifests into delays and pendency on the judicial side.[17] Therefore, administration and judicial aspect in judiciary need to be separated while maintaining the autonomy.

The phase 2 will be implemented in a decentralised manner. Committees will be made on 3 levels that is supreme court, high court and district court. They can have members from outside as needed though that happens rarely. Therefore, it is one the reasons for slow integration of the system.

PRINCIPLE FRAMEWORK

Access to expertise is a must if change is to be brought in Judiciary. Both short term and long term solutions are required. The judiciary needs to inculcate more branch specific people in the consultation process to make a user friendly design, ensure security and have an interdisciplinary approach of law and technology.

Response to Pandemic

The SC has issued guidelines[18] for adoption of technological solutions to each state according to the special needs and circumstances, considering the economic limitations too. The guidelines are to reduce the physical presence of all stakeholders and practice social distancing norms. All the high courts have been authorised to use video conferencing technologies to operate courts. It has been left upon the high courts to determine the modalities. Also grievance regarding technological impediments and its access, shall be registered on a helpline number. Evidence has to be recorded by the mutual consent of both

[16] Annexures, Objectives Accomplishment Report (n 51) 345- 346

[17] Pratik Datta, Mehtab Hans et al. 'How to modernize workings of courts and tribunals in India' (National Institute for Public Finance and Policy in India, 25 March 2019) <https://www.nipfp.org.in/media/medialibrary/2019/03/WP_2019_258.pdf> accessed 04 January 2021

[18] The Supreme Court of India, In Re: Guidelines for Court Functioning through Video Conferencing During COVID-19 Pandemic <https://main.sci.gov.in/supremecourt/2020/10853/10853_2020_0_1_21588_Judgement_06-Apr-2020.pdf> accessed 04 January 2021

the parties only. These measures were taken as an immediate step to continue access to justice for millions.

Constitutional Principles

While e-courts is way forward, it needs to be ensured that the constitutional rights are guaranteed to everyone. For the due process of law is of utmost important to ensure justice in good faith and equity.

1. Principle 1: Justice delayed is justice denied

Right to speedy trial is a fundamental right under article 21.[19] When the trial/judgement are delayed, it infringes upon the fundamental right of an individual. Constitution obligates the judiciary to reduce backlog of cases and increase its efficiency.[20] Therefore, technology is not just for immediate use but should be used even long after the pandemic. Faster access to justice is necessary and expedition of cases must take place.

2. Principle 2: Equal Access to all

Article 14 guarantees equality before law.[21] This equality should be maintained in the virtual world as well. Moreover, Internet is still not available to millions of people and digitalisation should be at par with the digital penetration so as not to handicap anyone from access to justice. Internet availability does not increase access to justice but familiarity with how the system works and its user-friendliness are also important.

3. Principle 3: Fairness and the process of law

The due process of law cannot be forsaken for expediating the process. One of the facets of due process is providing individuals immunity from unreasonable search or seizure of their papers, which ought to include information that is digitally maintained, for example on mobile phones or communication applications, without a warrant based on probable cause.[22] Also privacy of data which is not required by public or by courts should be maintained. It should be ensured that in no case the internal/ confidential documents of judiciary get to the public by unauthorized means.

4. Principle 4: Principle of Natural and Open Justice

[19] Hussainara Khatoon v Home Secretary, State of Bihar, 1979 AIR 1369.
[20] All India Judges' Association v. Union of India, (2002) 4 SCC 247.
[21] Art. 14, Pt. 3, Constitution of India.
[22] Kurt Wagnes, 'WhatsApp is at risk in India. So are free speech and encryption' (Vox, 19 February 2019) <https://www.vox.com/2019/2/19/18224084/india-intermediary-guidelines-laws-free-speech-encryption-whatsapp> accessed 19 April 2020.

E-courts could well lead to violation of natural justice. If one of the parties in physically present and other is connected virtually with video glitches and lag, this could lead to a bias to one physically present. Mechanisms to keep a check on this should be put in place.

Proceedings should take place in public is a well established principle of open justice.[23] *Constitution of India emits the spirit of open court principle by virtue of* **Article 145(4);** and **§.153B** of the *Code of Civil Procedure, 1908;* **§ 327** of the *Code of Criminal Procedure, 1973* .Proceedings should be live streamed generally so anyone and everyone who wants should have access to it. This requires a lot of data management and planning not just that but also right to fair trial of an accused should be upheld.

5. Principle 5: Privacy and Data Protection

As held by the supreme court, right to privacy is a fundamental right.[24] Some online video conferencing platforms may have leaked data for which the government then had to come up with certain guidelines.[25] Data protection is much needed, and adequate safeguards need to be placed. Cross border cyber attacks have also picked up during the pandemic to disrupt the systems and when a state organ is under such an attack, the stakes are higher and we should proceed with extreme caution.

Technological Principles

1. Principle 1: Open Source technology

Judiciary should use open source technology in conformation with international set practices. This not only lets the public scrutinise the software for any vulnerabilities but also is in consonance with open justice principle. Open source technologies are freely available which would also help in reduction of expenditure.

2. Principle 2: Security, evolution and resilience

Authentication of documents, digital signatures are important in any online medium. Adequate protocols should be in place as discussed before. With evolution of technology on an exponential rate, the technology in place should be capable of being replaced easily and should have area for improvements and evolution. The judiciary is too serving a population of more than 100 crore in various ways; Therefore, technological resilience is required. The

[23] Swapnil Tripathi v Supreme Court of India, (2018) 10 SCC 639.
[24] K.S. puttawamy v. Union of India, (2017) 10 SCC 1
[25] Mohul Ghosh, 'Govt Issues Strict Warning Against Zoom App; Says It's 'Not Safe', Issues Guidelines Of Usage' (trak, 16 April, 2020)

process of court is one of sanctity by law and needs to be uniform and transparent. Therefore, safeguards against cyber-attacks, data phishing etc. is a must.

Challenges of E-courts on ground level

In an interview with some lawyers it came forward, that internet connectivity has been the biggest issues of all. Secondly, system server capacity is low and all the cases for all the courts cannot be happen simultaneously. A lot of human intervention is required at various steps.

In criminal cases, multiple accused can't connect on the same network for video conferencing if placed in different jails. Moreover, police record is not digitalised, and their infrastructure needs to be upgraded. Therefore, a lot of work has to take place physically.

Even though master trainers for judges have been put in place 10 years ago, there is some kind of technological aversion. One point that came up is that advocates are also apprehending non-payment of fees by clients if thing go virtual therefore, they may keep pushing for physical hearings. A discussion with all the relevant stakeholders is a must to understand their aspirations and needs.

Conclusion

ODR were the first platforms, which laid down the path of E-courts. The developed nations have picked it up and are able to respond to the need of the pandemic. The Indian dream of E-courts started in 2005 but is still to see the light of the day. Internet connectivity, infrastructure, technological aversion are the biggest challenges. These challenges and issues need to be addressed. The pandemic needs to be seen as time for kickstart of a new era of where access to justice gets easier. Harmonising digital privacy and open justice principles would be a new challenge and creative technological innovations are required. Development of court systems and building adequate police infrastructure is required for courts to work. At the helm of affairs, is the need to separate judiciary from its judicial function with its administrative function to increase its efficiency.

There are a number of cases where technology has been a boon. Courts are able to decide upon matters of divorce when the litigants are sitting across 2 different countries.

"While technology has enabled us to go paperless in many courts and go digital, if not all the way then substantially, in many courts, we now have the benefit of modern artificial intelligence tools that will assist in improving the efficiency of our justice system through

sophisticated and contextual automation of existing repetitive non-judicial tasks and functions to reduce pendency, expedite judicial adjudication and create more time for judges to resolve complex cases."

- Justice Sharad Bobde (CJI), 2019

NTH ROOM CASE AND FIGHT AGAINST ONLINE SEXUAL ABUSE

Vratika Thakur[1]

Introduction

Although Covid-19 dominates the headlines worldwide, people in South Korea are enraged and traumatized by the news of the "Nth Room" online sex crime scandal. The nation is again facing an example of exploitation of women and misusing the global world of technology. South Korea was struck by the biggest criminal scandal in the Kpop business earlier in February 2018. The Burning Sun Scandal was an entertainment and sex scandal involving many celebrities, including Korean idols from famous K-pop groups and politicians, also known as the Burning Sun Gate. When singer Jung Joon-young admitted to secretly filming himself having sex with women without their permission on his KakaoTalk chatroom, the people involved were then charged with crime of rape and spy cams (called Molka which is a Korean term for secretly filmed videos of women). In less than a year, a blow was again dealt to the nation's public with the harrowing details of the Nth case where women were forced to share abusive videos of themselves on Telegram. The scale of people involved in this case has shown that many people still do not understand or care about the immorality of filming, viewing and distributing compromising images of women and children online without their permission even after the #MeToo campaign. In Korea, the crimes echoed broader problems, such as the on-going spy cam outbreak in the country and the misogynist ideology of people deeply entrenched in the society. As the nation continues to struggle to resolve the on-going spy cam (Molka) epidemic, these crimes mirror a larger problem in Korea. It reflects the misogynist ideology of people deeply entrenched in the society. The nation now needs to confront this toxic blend of technology, sex and crime that its structures has failed to prevent.

What is the Nth Room ?

The Nth Room is a mass digital sex scandal that took place in South Korea, using the Telegram chat messenger, perhaps one of the biggest and most widespread that the country has ever encountered. At least 74 victims, including minor children were forced to upload graphic and sometimes violent videos of their own into social media chat rooms and telegram communication applications.[2] These chatrooms were accessed by at least 260,000 users and

[1] LL.M Student GujaraT National Law University, Email id – thakurvratika@gmail.com
[2] Nicole Desouza, 'The Nth Room case and modern slavery in the digital space' (*The Interpreter*, 20 April 2020)

paid for with either their own crypto-currency or additional videos. More than 220 individuals suspected of digital sex crimes were arrested by the police and Cho Joo Bin, their ringleader (the main defendant who went by the code name Doctor), was charged.

In order to commit the crimes, the perpetrators relied on the Telegram software that uses encrypted messaging. Women targeted for the Nth Room were regularly contacted online via other social media sites including Twitter before being encouraged to move future communications to Telegram. Because of its broad measure of authentication and encoding, the app is renowned for being untraceable. Applications like Telegram have a new means of messaging, linking and using blockchain to ensure that the violence by crime syndicate is paid for. With the help of the app, 25-year-old Cho Ju-Bin, who is currently under investigation, enabled the company to sell sex videos to an online audience. Cho created a number of chat rooms with the aid of a tier ranking: 1st floor, 2nd room, 3rd room..... Nth room, since the exact number of rooms created to circulate this terrifying crime is unknown. To gain entry to these chat rooms, users were willing to pay a significant sum of money, and the amount of money paid determined the number and type of room to which one could gain access. The room with the lowest tier ranking was stated to have an entrance fee of $80 USD, while users who charged $1,200 USD would have access to the rooms with the highest tier rating.[3] The lowest-ranking rooms had access to 'fewer' abusive videos, and the users who paid the most accessed the room with the 'most' abusive videos. More than 260,000 individuals are said to have joined the Nth Room party, with their clientele including prominent entertainers and artists, athletes, CEOs, etc. It falls, as defined by the UN, very much into the category of "human trafficking and modern slavery".[4]

In the scandal, 76 female victims have been identified, with teenagers being the main target. 12 of them were minors and it was confirmed that the youngest victim was about 9 years old. According to the BBC[5], an alleged survivor still in school described how, while looking for work online, she was asked to submit photographs of herself and later at least 40

https://www.lowyinstitute.org/the-interpreter/nth-room-case-and-modern-slavery-digital-space accessed 20 March 2020

[3] Shreya Juyal, 'Internet, Sex Crimes and How Technology Failed Women: The Nth Room' (*Du Beat* 19 April 2020) https://dubeat.com/2020/04/internet-sex-crimes-and-how-technology-failed-women-the-nth-room/ accessed on 12 Januay 2021

[4] Nicole Desouza (n 1)

[5] Laura Bicker, 'Cho Ju-bin: South Korea chatroom sex abuse suspect named after outcry' *(The BBC*, 25 March 2020) https://www.bbc.com/news/world-asia-52030219 accessed on 30 December 2020

sexually abusive images. "He had my face, my voice, my personal information already," said the survivor. I was scared that if I said I would leave, he would threaten me with that detail".[6] An anonymous victim explained how she had no idea what Telegram was in an interview with the Korean radio program CBS[7], but the person hiring her asked for her bank account information, address and phone number after downloading it. She was slowly forced to take pictures and make graphic videos, using her personal information as threats against her, even though she was still in high school at the time.

Up until now, there have been more than 100 offenders arrested. The bulk of them are young men below 40. The exact nature of these alleged crimes is unknown, but there were 260,000 users of 56 monitored chats on Telegram, according to the Korea Cyber Sexual Abuse Response Centre.[8] This case shows to what degree digital technology can be used in a new form of modern slavery for the virtual abuse of people. As described by one of the victims, her identity and personal information, so much of which is freely shared on social media as part of everyday life, can be turned into trapping someone in an exploitative relationship.[9]

The frustrating reality is that while the Telegram chats use a fresh medium, the tactics of the men and their dehumanization of the women are oppressively familiar. Soranet was also one such website full of spycam videos of women, and which also offered an invitation in real time to rape women. It was shut down in 2016, but similar websites cropped up before and after it was closed.

Online discussions in South Korea show that some continue to find it understandable to share these clips and images because men want to watch such material "naturally." In South Korea, the persistent use of date rape drugs and molka indicates that toxic masculinity has not diminished. Felicity Gerry, a criminal law barrister and professor at Australia's Deakin University who has prosecuted human trafficking, said:

[6] ibid
[7] Ron Kim, 'Victim Of Telegram Nth Room Case Speaks Up About The Horrors She Faced As A Middle School Student' (Koreaboo, 24 March 2020) https://www.koreaboo.com/news/victim-telegram-nth-room-case-speaks-horrors-faced-middle-school-student/ accessed on 30 March 2020
[8] Suhyoon Lee, 'South Korea's latest sex crime scandal is a blackmail ring streaming abuse on Telegram' (*Quartz* 24 March 2020) https://qz.com/1824130/korea-shocked-by-telegram-chat-room-sexual-abuse-scandal/
[9] Laura Bicker (n 4)

"The idea of enslaving people is not new and the concept of organized crime is not new to keep the practice a secret. However, the use of technology enables this to be achieved in new ways, both to conduct the crime and to avoid investigation."

Gerry said the "shame factor" is mostly used by the offenders to pull a woman in[10]. Let's say that a woman wanted to be a model, so she provides a nude image for that purpose. Then the suspect will say,' We can either put it online so that anyone can see it or your family can see it' and that can be devastating, particularly in some cultures. From afar, they can be controlled, exploited and harassed. The Nth room case used a similar design. Young students and minors in need of part-time work and offers were pressured to share their personal and financial information and were later used to compel them to execute and document chat room activities. With advancements in technology, the methods used to control people have evolved; the fundamental issue, however, remains constant.

Not a One Nation Problem

Modern slavery is a broad term used to describe situations where abuse, deception or coercion is used by others to exploit the victims and take away their freedom. It covers global crimes such as human trafficking, sexual exploitation and forced labour. According to a joint study by the UN International Labor Organization and the Walk Free Foundation, 71 percent of global slaves are female.[11] When looking specifically at forced sexual exploitation, women or kids are the victim majority of the time.

In South Korea, digital sex crimes are notorious for attracting light sentences, including those involving girls. Child porn offenders can be sentenced to life under Korean law, but in fact, the Ministry of Gender Equality and the Family reported that the average was only two years in 2017. Son Jong-woo, the creator of one of the world's most notorious child porn websites received 18 months in jail.[12]Korean institutions are unable to catch up to rectify this horrifying practice. Law enforcement is more reactive than proactive, frequently forming task forces after splashing through the media following a scandal. As many criminal activities take place on foreign servers and platforms, collaboration with governments internationally is still a lagging process.

[10] Nicole Desouza (n 1)
[11] Walk Free Foundation, 'Global Slavery Index 2018' (*Mindoro Foundation* 2019) https://www.globalslaveryindex.org/ accessed on 30 March 2020
[12] Haeryun Kang, 'Another digital sex-crime scandal leaves South Koreans reeling — and waiting for justice' (*The Washington Post* 11 July 2020) https://www.washingtonpost.com/opinions/2020/07/10/another-digital-sex-crime-scandal-leaves-south-koreans-reeling-waiting-justice/ accessed on 30 March 2020

South Korea is not the only country that is fighting with cybersex crime. China started investigating domestic websites containing child pornography in the aftermath of the coverage of the Nth Room. The websites have deliberately installed servers abroad in a bid to avoid local authorities, so that when one site is taken down, it can easily re-emerge under a new name.[13] Another research on Australians paying to watch live videos of sexually abused children in the Philippines was published in February by the Australian Institute of Criminology.[14] Due to factors such as powerful internet coverage and relatively low cost, English language skills, and poverty, many rights organizations have described the Philippines as a hub for live streaming child violence. The study analyzed the characteristics of offenders using the sites and found that two-thirds of them were men in their 50s and 60s. Over a 13-year period, more than 250 Australians spent $1.32 million on watching child sex abuse online. More than half of those individuals had no criminal records recorded.

For digital sex offenders, punishments need to become more stringent. It isn't enough to look at precedents for sentencing guidelines. Digital sex crimes are unprecedented; new definitions and new guidelines are needed. Changes are steadily coming. There is a palpable concern, especially among women, that the perpetrators will not get what they deserve. The concern seems valid: recently, one of the developers of the original nth rooms was sentenced to 42 months in jail.

But stricter penalties alone won't be adequate. The uncomfortable reality that sexual dehumanization of women is widespread beyond the nth rooms must be addressed by global society: in classrooms, workplaces, politics and everyday life's apparently innocuous behaviors. "Feminism conversations must go beyond "these women hate men" or "men are also suffering; feminism is just reverse discrimination against gender. Schools need to actively educate learners on why gender sensitivity is critical, particularly young men.
Digital sex offenses are global issues, but the effort to combat the epidemic is one of constant diligence. Forensic mechanisms are more sophisticated than they used to be, as Gerry notes, but offenders are still innovating. The criminals are adapting to the changes, as they have forever.

[13] Ji Yuqiao, 'Amid South Korean Nth Room case, Chinese drama delves into violence against women and sexual abuse' (*Global Times* 29 March 2020) https://www.globaltimes.cn/content/1184122.shtml
[14] Rick Brown, Sarah Napier & Russell G. Smith 'Australians who view live streaming of child sexual abuse: An analysis of financial transactions' [2020] Australian Institute of Criminology

There is a movement towards more stringent punishments that would label and prosecute those who knowingly consume pornographic content as sex offenders. Korea's centralized education system needs to move on, following rising public awareness, including the landmark women's rallies against spycams in 2018. The sex education of the nation also attracted criticism for being discriminatory; suggesting that in schools as well there is a widespread lack of gender sensitivity.

Measure to counter online sexual exploitation and abuse

Law enforcement investigations are among the most popular ways of preventing online child sexual exploitation and harassment. For investigating online child sexual abuse and harassment in the cyberworld, federal, global, and foreign law enforcement agencies track and collaborate together.

The existence of harmonized national legislation, international cooperation in criminal matters, such as mutual legal aid and extradition, bilateral, regional and multilateral conventions and agreements on sexual exploitation and abuse of children, and the effective implementation of such laws, treaties, conventions and agreements, make it possible for agencies to collaborate and cooperate in international investigations of child sexual exploitation.[15]

In order to track, investigate and prosecute perpetrators of sexual assault and exploitation of children online, undercover law enforcement operations are also carried out. The undercover operation of the *Kids the Light of Our Lives* Internet chatroom, which acted as a live streaming platform for child sexual abuse and the downloading and dissemination of child sexual exploitation and abuse content is a case on point.[16] Undercover law enforcement officers, who were part of the Virtual Global Task Force (a task force made up of various law enforcement agencies around the world, whose ultimate aim is to create partnerships with other non-member law enforcement agencies and the private sector to tackle online sexual harassment and abuse of children), were able to penetrate the chatroom and collect critical

[15] Paul Baines, 'Death and Best Interests' (2008) 3(4) Clinical Ethics < https://doi.org/10.1258/ce.2008.008040> accessed 30 March 2020

[16] Victoria Baines, 'Online Child Sexual Abuse: The Law Enforcement Response' (World Congress III against the Sexual Exploitation of Children and Adolescents, Rio De Janeiro, 25-28 November 2008)

evidence that was used to successfully prosecute the chatroom host and the people who used the site.[17]

Private sector partnership with government agencies is also a key to counteracting online sexual abuse and bullying of children. This relationship involves "blocking" links to websites often accessed and used by children and even by registered child sex offenders without the knowledge of the former. A case in point is the 2012 Operation Game Over, where "Microsoft, Apple, Blizzard Entertainment, Electronic Arts, Disney Interactive Media Group, Warner Brothers and Sony" from online video game sites took down "more than 3,500 accounts of New York registered sex offenders" (e.g., Xbox Live and PlayStation).[18] In order to harmonize and monitor child sexual abuse practices and online content harassment, private businesses have also collaborated to create an Industry Hash Sharing Network ('a cloud-based hash sharing tool').[19]

Databases where content on child sexual abuse can be submitted for investigative purposes have also been created, such as the International Child Sexual Exploitation (ICSE) database of INTERPOL, to tackle online child sexual exploitation and abuse. These databases not only help identify children who have been exposed to sexual abuse and violence, but also help track and convict perpetrators. For instance, the leader of a network of sexual offenders in Japan was discovered when authorities in Denmark and Australia uploaded videos of an unidentified child sexual abuse victim to ICSE.[20] Like the ICSE database, the content in this database is used to identify victims and perpetrators of child sexual exploitation and abuse, and to prosecute child sexual abusers, information for child sexual abuse, and child sexual exploitation and abuse facilitators can be provided. In the United States, the Child Victim Identification Network of the National Centre for Missing and Abused Children (NCMEC) acts as a central centre for information on child sexual abuse.

[17] ibid
[18] Office of the Attorney Journal, 'A.G. Schneiderman's "Operation: Game Over" Purges Thousands Of Sex Offenders From Online Video Game Networks' (2012) https://ag.ny.gov/press-release/2012/agschneidermans-operation-game-over-purges-thousands-sex-offenders-online-video accessed on 30 March 2020
[19] Nikoleta Lydaki Simantiri, 'Online child sexual abuse and exploitation' (2017) https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2018/10/Revue-OCSE_ANG-min.pdf accessed on 31 March 2020
[20] European Commission, 'Towards a Global Indicator on unidentified victims in child sexual exploitation material' (*Interpol*, 2018)

The sheer size of the internet, and the number of online platforms and applications on the market, and new technology on the market, make it easy for criminals to hide in the open. Given the amount of data and the number of web outlets, conventional investigative approaches of child sexual exploitation and violence are not enough. New technical innovations will reduce the time it takes to identify perpetrators and victims, and will be able to proactively mitigate child abuse and sexual exploitation content. For example, Terre des Hommes, an international child protection agency, has created "Sweetie," a virtual ten-year-old Philippine girl designed to recognize and communicate with sexual offenders online to publicly expose them and alert suitable law enforcement agencies, in collaboration with partner organizations.[21] Web crawlers[22] (i.e.' an application that traverses the World Wide Web systematically and continuously for a specific purpose') and data mining (i.e. "extraction of valuable knowledge from vast data sets;")[23] techniques have also been used to proactively track online child sexual assault and violence. Cases in point are devices that are part of the Defense Advanced Research Projects Agency (DARPA) Memex project, such as DIG and TellFinder, incorporating web advertising, downloading material, finding links to downloaded content, and applying the information collected to a database that is query-enabled.[24] This approach is meant to identify the victims and those responsible for sexual assault and other crimes. Traffic Jam, which identifies pattern in online content and recognize victims through the use of facial recognition technology was also developed by Marinus Analytics.[25] Many resources concentrate on identifying victims depicted in the content of online sexual harassment and violence by concentrating on the past and background of the victim in the content in an effort to locate an item in the material that might provide details about the location of the victim (e.g., the "Stop Child Abuse - Trace an Object" campaign of Europol).

Some technical steps taken by law enforcement authorities to carry out inquiries into child sexual exploitation and violence are considered controversial. In the U.S., for instance,

[21] Terre des Hommes, 'Webcam Child Sex Tourism Becoming Sweetie: A novel approach to stopping the rise of webcam child sex tourism'[2013] Terre des Hommes 11
[22] Andrew Butterfield, Gerard Ekembe Ngondi, and Anne Kerr (eds), *A Dictionary of Computer Science* (7th edn Oxford University Press 2016)
[23] Nigar Hashimzade, Gareth Myles, and John Black, *A Dictionary of Economics* (5th edn Oxford University Press 2017)
[24] Cheryl Pellerin, 'DARPA Program Helps to Fight Human Trafficking' (*US Dept of Defence* Jan 4 2017) https://www.defense.gov/Explore/News/Article/Article/1041509/darpa-program-helps-to-fight-human-trafficking/ accessed on 30 March 2020
[25] ibid

law enforcement agencies may "rely on established software vulnerabilities or build tools to identify and use previously identified and unrevealed vulnerabilities (or otherwise obtain exploits for such zero-day vulnerabilities) that they can then use" to gain access to criminals' digital devices and the information they contain.[26] These techniques are "specially designed exploits or malware," known as Networking Investigative Techniques (NITs), which have been used in many visible web and Darknet investigations of child sexual abusers and child sexual exploitation materials[27] For example, in Operation Playpen, which targeted (at the time) one of the largest Darknet sites containing child sexual abuse content, "the NIT used by the government was malware that was suddenly distributed through a secret Tor service".[28] Through (apparently) exploiting a loophole in the Firefox web browser (running as part of the Tor browser) to place computer code on computers that would send private information to a law enforcement server outside the Tor network, the malware was designed to penetrate the privacy provided by the Tor network.

The reality is that a multi-faceted approach is needed to effectively tackle online sexual harassment and violence, which includes not only law enforcement strategies, coordination of services given to victims of sexual assault, cooperation between all sexual harassment organizations, and educational programs and awareness campaigns addressing these crimes and Internet protection but also certain precautionary measures need to be taken by women and adolescents to ensure their safety while being online. Some basic steps that can be followed are mentioned below:-

1. Avoid sharing passwords.

A trusted friend or partner might have shared their password. According to the Norton CyberCrime Study[29], two in three individuals think it is more risky to share their email address with a friend than to lend them their vehicle. Fear is logical and fair. While friends do not cause harm deliberately, they expose passwords to others accidentally. Relationships change before the password does, often. Hold those passwords that are vulnerable and complicated.

2. Don't leave the device's webcam connected

[26] Kristin Finklea, 'Dark web' (CSR Report 2017) 1 < https://fas.org/sgp/crs/misc/R44101.pdf> accessed 30 March 2020
[27] Kristen Finklea (n 23) 1-2.
[28] Thomas Brewster, 'Exclusive: What Happened When The FBI Took Over The Instagram And Kik Of A Child Porn Dealer' (*Forbes* 6 March 2019)
[29] The Harris Poll, '2019 Cyber Safety Insights Report Global Results' (*Norton Life lock* 2020)

There are so many gadgets that, without the person's knowledge, can turn the device's camera on and capture all the private movements. Disable camera permission as a precaution and, when not in use, keep the camera lens closed or protected

.

3. Don't share any private information.

Relationships have only two shades, very good or very bad, in a continuum. From one end of the spectrum to the other, even people at their best can swing. If a person shares private messages, pictures, documents or something that has the power to come back and embarrass them, use caution. Very often sinister individuals look on social networking platforms to make friends with naive individuals. Care should be taken when posting information on personal lifestyle and whereabouts. In order to find ways to get to the victim, stalkers can use a simple image or status update. Disable Geotagging in-camera. Enable only when necessary. At any given time, any device that has an active 'location service' is likely to disclose the victim's exact location.

4. Secure your devices with anti-virus software and keep them updated

It's like sitting in a house without a surveillance system with the doors open to get a mobile phone or laptop. Android and mac computers are all at risk of breaching and taking over your life with malware. A secure security system is also mounted on all your computers.

5. Read the fine print

The user should now and comprehend the privacy policy of any corporation that they use and its terms of service. Some websites are able to own, sell, rent or resell the data to whoever they want. This will come back as a bigger question, and since the user has agreed to the terms, the law will not be able to protect them.

6. There is no such thing as 'freebies'

In the form of sports, offers, promotions, etc., freebies come. They can get infected with malware, spyware, and viruses. These can enter into the computer and own all the data that is present there.

7. Block any person that you don't want to interact with

Never feel odd refusing requests from individuals you barely know. You should choose who will remain on your friend list. The first line of defence when it comes to security, both

online and offline, is common sense. If you sense like something is wrong, go with your instincts and take a step back, block them and immediately seek support.

Conclusion

Each year, an unacceptable number of women fall prey to cybercrimes. The scope of the Internet and the rapid distribution of information through mobile devices have created new possibilities that could endanger lives of women and adolescents, so it is important to be aware of the dangers. There needs to sensitization about online abuse, safeguards against possible dangers and strict sanctions against anyone who indulge in such illegal activities. Once crime has been committed protective measures and support for victims of online abuse must be in place. The government needs to set up effective social services and multidisciplinary systems to provide the victims, their close relatives and those responsible for their care with the appropriate resources. The establishment of information systems, such as telephone or Internet help lines, which are capable of maintaining security and privacy for victims, should be encouraged and funded. For their physical and psycho-social rehabilitation, victims should also be provided with adequate therapy. At early stages adolescents and minor should be made aware about potential dangers on online platforms and be taught about safe usage of internet through various educational programs.

CYBER TERRORISM: A GLOBAL SECURITY THREAT

Lahama Mazumdar[1]

Abstract

This paper attends a very important issue for cybernetic security system in the context of knowing measures, warnings, and proofs of cyberterrorism. The discussion continues with analysing on whether the International community has legally recognised the threat that a deviant globalisation may pose, furthered with a vivid discussion on incidents of cyber terrorism, tools of terror attack and methods of cyber terrorism. Prolonged violations of human rights have led to the urge of violence among suppressed groups. Modernisation of technology has eased communication but has also opened new doors for the attackers who not only transfer funds easily but can also provide military and paramilitary training online. What is debatable is how far has the globalisation succeeded or progressed in suppressing the incidents of cyber terrorism and whether globalisation itself could extend a helping hand in curbing such cyber nuisance and threat to the world. Last but not the least the paper also tries to analyse the domestic initiatives of India, the approach of multinational and regional organisations in curbing cyber terrorism.

Globalization hints towards the mix of business sectors in the worldwide economy, prompting the expanded interconnectedness of national economies. It has led to free movement of goods, capital, technology, service, people. Globalisation is reflected in Economic growth, Social development, cultural development and various other factors. Although the above-mentioned factors are of paramount importance in governing globalisation, there is one aspect to it, which has connected all these arenas, i.e., technology or the cyber networking. Communication over internet has made global development stronger and more widespread.[2]

However advantageous the proposition may seem, but some disadvantages still exist. Convergence is one of the darkest sides to globalisation. A special kind of this convergence is emerging in the cyber world where the level of threat is high and our level of preparation is low. World's server has become one of the threat packages where billions of worth's cyber crime occur every year. In the present world cyber terrorism is the stressing pattern in parallel to globalization. The new wave of globalization sponsored by present day innovations is confronting colossal feedback. Pessimists of globalization argue that globalization supported

[1]

[2] Chandan Sengupta, *Conceptualising Globalisation*, 36 ECON. POLIT. WKLY. 3137–3143 (2001), https://www.jstor.org/stable/4410994.

by tech savvy terrorists has enabled the terror organizations to exploit communication systems, information and funds etc. to further their activities. Cyber capability and its cash convergence with the terrorist groups can make the risks of catastrophe higher. [3] Incidents of cyber terrorism is on a notable rise starting from Internet Black Target in the year 1970, Kosovo Attack, and the infamous Trade Center attack of 9/11. India has also been at the receiving end of the problem with the incidents of 2008 serial blasts in Varanasi and then the 26/11 attack in Mumbai.

The decentralised, difficult to control and easily accessible medium of cyber networking has made it a direct or an indirect medium of connect and usage for the terrorists. Military and civilian defence networks, government networks, networks used for business or any sort of communication, any network used to control public utilities can all be subject to violence of terror attacks.[4]

With Globalisation being dominated by the western industrially advanced countries like United States and Japan, Islamic Countries have been challenging their dominance by means of these several violent assaults. The networks of these transnational terrorists are also operating at the context of Globalisation.

DEFINING CYBER TERRORISM

Cyber whiz Barry C Collin was the first person to invent the term CYBER TERRORISM. According to him cyber terrorism was mainly about the coming together of terrorism and cybernetics.

In this paper the researcher would like to quote the definition given by Professor Dorothy E. Denning. She makes a statement before the Special Oversight Panel on Terrorism, where she says " Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as

[3] James Stavridis, How Terrorists Can Exploit Globalization, The Washington Post, 31st May,2013, (June 1, 2020, 2:31 PM) https://www.washingtonpost.com/opinions/how-terrorists-can-exploit-globalization/2013/05/31/a91b8f64-c93a-11e2-9245-773c0123c027_story.html?utm_term=.1c0364708a8c

[4] Aviv Cohen, *Cyberterrorism : Are We Legally Ready?*, 9 J. INT. BUS. LAW 1–40 (2010), http://law.hofstra.edu/pdf/academics/journals/jibl/jibl_vol9no1_cohen_cyberterrorism.pdf.

cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not . "

The United States Federal Bureau of Investigation (FBI) defines terrorism as, "The unlawful use of force or violence, committed by a group(s) of two or more individuals, against persons or property, to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives." [5]

The main component of the definition of cyber terrorism is about committing of a criminal act using cyber space as a media. It causes violence, death, injury and also creates terror in the mind of the victim and can also coerce the government by using these means to change its policies. It can attack the defence system of a country. It leads to the creation of fear in the minds of the people which helps these terrorists to fulfil their religious, social and economic goals.

Looking at these definitions one gets very clear of the notion that the definition of cyber terrorism embeds into it the definition of terrorism. Both the terms are interconnected with the indulgence of cyber networking in the former definition. The impact of both cyber terrorism and terrorism is on the same lane where the effect is faced by the general public by means of damage to life or property. Terrorism has just been influenced with the development of time where the growing influence of cyber space as a medium of communication which has led to serious losses faced by countries and communities.

INSIGHT TO CYBER TERRORISM

INCIDENTS OF CYBER TERRORISM

The history behind cyber terrorism is not that long though the past decade has witnessed many cyber security threats. Financial institutions, governmental defence systems, transportation, telecommunication have been one of the common targets who have faced the

[5] Mitko Bogdanoski, *Scienti Þ c article CYBER TERRORISM – GLOBAL SECURITY THREAT*, INT. SCI. DEFENCE, SECUR. PEACE 59–72 (2011).

cyber-attacks. To discuss the major incidents, one cannot forget the incident of Gulf war where Iraqi hackers had disrupted the troops deployed there. Then comes the year 1994 when the U.S defence system was majorly attacked. In 1997 US saw another attack where the US power grid was attacked where all the command and control systems were silenced by usage of hacking tools. In 1998 another attack happened where millions of people could have lost lives where the controls of the Roosevelt dam in Arizona , USA was hacked where flood waters when released endangered millions of lives. 1998 saw another Spanish incident where mail bombings occurred and Institute of Global Communications had thousands of spam emails sent to them . The protestors wanted them to shut down their webpage which was said to have materials of a terrorist group. Eventually the website had to be pulled down due to this incident. The same year then recorded the activities of the Internet Black Tigers where they had threatened Sri- Lankan embassies with 800 emails a day to disrupt their communications. All the computer systems could be jammed and a serious threat to the security of the country could have happened.

In the year 1999 Kosovo conflict became worth mentioning where NATO computers were bombarded with email bombs and were hit by denial of service attacks. Academic institutions, financial organisations, public institutions received virus containing emails which effected their normal day of work. [6]

Another incident worth mentioning is the September 11, 2001 terror attack where the lack of readiness of the American forces to deal with cyber terrorism was discussed. Office of cyber space security was constructed after this attack to make the defence forces ready to combat these kinds of threats caused by cyber catastrophes. Cyber terrorism had become a tool of bloodshed for the terror organisations where launching missiles and all sorts of communications had become so easy that a click of a mouse could facilitate it. It had on a large scale disturbed and effected the national economy. [7]

Even in the 26th November 2008 Mumbai blasts where coordinated shootings and blasts resulted in deaths, traces of cyber terrorism was found where the mode of communication among the wanted and the other terror organisations was based on voice over Internet Protocol. E- Governance and E-commerce have increased India's development but at the

[6] Rohas Nagpal, *Cyber Terrorism in the Context of Globalization*, II WORLD CONGR. INFORMATICS LAW 1–23 (2002), http://www.ieid.org/congreso/ponencias/nagpal, rohas.pdf.
[7] Susan W. Brenner, *Cyberterrorism*, 29 MEDIA ASIA 149–154 (2002).

same time it has made it vulnerable by the threat to paralyse the economic and financial institutions. Various research papers reflect that with the new currency ban that had happened in the year 2016 a lot of cyber-attacks had happened showing vulnerability of the banking sectors. Debit cards issued by SBI, Yes Bank, ICICI bank and several others had compromised with the cyber-attack that happened in October, 2016. [8]

These several incidents shows the problems and instances that have been faced by the defence and the financial institutions due to globalisation and development of communication technology.

METHODS OF ATTACK

Before going into tools of attack one needs to be aware of the methods of attacks where we see mainly viruses and email bombs were the most common medium of attacks. There are three main methods of attack. *Firstly*, Physical attack where old methods of fire and bomb are used to break the computer infrastructure; *Secondly*, Syntactic attack where Trojans and viruses are used to make the system unpredictable and uncertain where delay is caused in the computer system thereby breaking into the computer infrastructure; *Thirdly*, It paralyses the computer infrastructure by means of playing with the users confidence where the information provided by the user is modified without his knowledge and fed into the system whereby user looses all his control in the system per se. [9]

TOOLS OF TERROR ATTACKS

Certain tools are then used to effect the computer systems. They are:

- **Hacking** : Packet sniffing, password cracking are the most widely used techniques in this tool. It leads to an unauthorised access to the computer system belonging to someone else. The user then becomes vulnerable as the control is lost on the system.
- **Trojans**: This tool is a deceptive program where the program is installed for doing something but it ends up doing something else.

[8]Smt Saheli Naik, *A Biggest Threat to India – Cyber Terrorism and Crime*, 5 QUEST JOURNALS ,JOURNAL RES. HUMANIT. SOC. SCI. 27–30 (2017), www.questjournals.org.
[9]*Id.*

- **Emails**: Emails are used to threaten , defame and for disseminating false information . They are also often host to worms and viruses attacked to them where it can corrupt the computer.
- **Denial of Service** : This is a very common problem which has increased the vulnerability of the defence and the banking sectors of India where the authorised people cannot access their networks and somebody else accesses it thereby aiming to cause loss of people and property.

With the increasing amount of tools the threat to national integrity, security has been increasing. [10]

CYBER TERRORISM: AN INESCAPABLE OUTCOME OF GLOBALISATION

This part of the chapter analyses the link between globalisation and it suggests that globalisation might be the reason for escalated amount of terrorism. There is an involvement of rule of law and human rights violation which have come up to support this point. Prolonged violation of fundamental rights is injustice and it leads to surge of violence among the suppressed group of people. Ben Clarke in one of the chapters of the book " responding to terrorism" tried to create a nexus between Globalization, technology and terrorism which the researcher finds to have extreme amount of importance while linking it to cyber terrorism. He says that with modernisation of technology sending funds across the world has become easier. Cyber space has so much power that it can in itself become the sole source of communication between terrorists. Not only fund transfer but it has also facilitated sending of messages which are encrypted and hard to decrypt , also training to military and para military forces are provided via these technologies. Islamic groups have used such communication methods in coordination between them to plan a terror attack. It has become easier for terrorists organisations to make their opinions vocal via internet and also influence public opinion based on that. There has been several incidents accounting to religious and ethnic violence . Post colonial era brought around more of such incidents . One can take the example of India where it is easy to observe that India faced serious incidents of violence post to it getting independence from Britain in 1947. British intruders had took the most powerful method of divide and rule by which it was successful to get control over India, but that in turn had created a rift between the religious and ethnic people. Though British invasion had in

[10] S.S Raghav, *Cyber Security In India's Counter Terrorism Strategy*, http://ids.nic.in/art_by_offids/Cyber%20security%20in%20india%20by%20Col%20SS%20Raghav.pdf

turn brought globalisation in terms of new structure of education, administration, governing methods in India , but it did extinguish a lot of traditional customs and laws whose restoration post Independence had become impossible. Partition brought in violence and terror, post to which religious violence and terror has been a continuous process in India. Power hungry politicians and rival groups have become the fuel to such terror activities in India. Though these challenges were huge but still the economic growth of India has been substantial. Globalisation in turn has also improved the living standard of people which in turn could also be the reason behind declining terror violence but that is only a farfetched idea of the researcher. Noting the terror activities post colonisation due to differences between ethnic and religious group one ant ignore the violation of human rights and international rule of law by these activities. The terror organisations have repeatedly ignored the human rights of the victims and also have rejected the idea of democracy. Globalization has its own profits and losses . It has influenced the living standard of people but it in turn has also increased the tools for dispersal of Islamic ideas of terrorism. Blocking access to such terrorist groups is not possible which in turn has increased stances of changes in ideology of people. Security measures in Education and impartation of knowledge needs to be adopted which in turn an act as a way of shaping young minds with values of rightful justice, mercy, compassion and kindness. Globalization definitely has a lot of costs to bear but it also has given lots of measures to limit such differences between groups. International Forums have been built to deal with such differences between groups. The UN Charter in its chapter VI[11] has discussed peaceful methods of resolutions of such disputes which includes measures like arbitration , conciliation and judicial settlement of such disputes which in turn has a effect in controlling such events of destruction. [12]

LEGAL ISSUES AND DEFENCES IN INDIA

INDIA - DOMESTIC INITIATIVES

Certain organisation in India were brought to existence to bring in cyber security. The researcher came across four of such organisations. First, "National Information Centre (NIC)" which was brought to existence to provide a backbone to the governments to regulate e governance and protect it from any kind of cyber attack. Second, "Indian Computer

[11] *Pacific Settlement of Disputes,* United Nations (2017), http://www.un.org/en/sections/un-charter/chapter-vi/index.html
[12] Benjamin Clarke, Robert Imre & T. Brian Mooney, Responding to Terrorism 129-155 (2009).

Emergency Response Team (CERT IN)" which mandates the security of cyber space to ensure that communication and network infrastructures are not affected. Thirdly , " National Information Security Assurance Program (NISAP)" this organisation was created by CERT IN to establish a link between government and critical infrastructures thereby protecting both. Fourthly, " The National Association Of Software And Services Companies (NASSCOM)" was brought to existence by the Indian Information Technology sector to help the BPO sector and software technologies.[13]

DOMESTIC LAWS

Section 66 F of the Information Technology Act, 2000 has put forward a provision which has made cyber terrorism punishable with imprisonment up to life sentence. It provides that-

" *any person with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people causing denial of access to computer systems to persons authorised to access, to penetrate a computer without authority or to contaminate a computer system which creates the likelihood of destroying the property or services essential to life or destroy the supplies or adversely affect the Critical Information Infrastructure or creates danger to life or injury to persons* " is committing cyber terrorism.

Section 66F (1)(b) provides-

" any person knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism."

Another important section which finds importance is section 70(B) of the IT Act, which lays down about the formation of CERT IN which has already been stated above.

[13] Naik, *supra* note 8.

This was purely the reiteration of the concept provided in the bare act, but the matter of importance is the fact that after the 2008 amendment of the IT Act , the ambit has increased with respect to electronic signatures replacing digital signatures making electronic records more relevant and reliable. The fact that now physical documents and electronic documents are treated at par has helped retain the sanctity of this legislation. Karnika Seth , a prominent author in the field of cyber crimes has also expressed her opinion on the need of India to sign a International Convention on Cybercrime . India has now already seen several attacks related to cyber terrorism and it has also seen the power of this attacks to control the financial and the defence system of this country. It is earlier already stated in this paper the several instances where India faced the brunt of this crime so it is quite justified when one looks at the viewpoint of the prominent author. [14]

There is also a lot of executive approach to this concern. By-laws and regulations have been passed by state governments for effective implementation of the IT Act. There has been implementation of laws by Karnataka where there has been rules made for cyber cafe's to regulate the information of people accessing their resources where they have to keep in record information about details like photo identity, time of usage of their user's.[15]

RECOGNITION BY INTERNATIONAL COMMUNITY

Legal inadequacies have always been the reason why criminals get away with the heinous crimes they commit. Though cybercrimes only occur in cyber space, these crimes have far reaching effects which can lead to loss of life and property. Being a crime, which has spread beyond the physical boundaries of states there is always a need of international harmonisation of laws to fight this menace. There have been not only international but also regional agreements that have been made on the same.

UNITED NATIONS

- **"Commission on Crime Prevention and Criminal Justice (CCPC)"-** This unit of United Nations has made several trials to prevent and control computer related crimes so as to tighten the security related to cyber space. Close harmonious relations between countries is one such approach suggested. UN Crime Congress has considered this accordingly.

[14] Karnika Seth, Computer, Internet and New Technology Laws 362 (1 ed. 2013).
[15] Information Technology (Karnataka) Rules 2004, Rule 2-4.

- **"United Nations Convention against Transnational Organised Crime"** - Central assembly made attempts to adopt this and finally in 2000 it became successful in doing so. However, what was unique about this was that routine computer crimes did not come under its coverage, only crimes committed by gangs like that of cyber terrorists could be caught by them.[16]

INTERPOL

The speciality of this organisation is that it works when there is no diplomatic relationship that exist between countries. Fusion Task Force is this anti-terrorism section that is created by this organisation, which does the work of identifying such terror groups, collecting information regarding them and then helping the member countries to then address the problems regarding this. [17]

MULTI NATIONAL ORGANISATIONS

- **"G8 Group" :** It first started its fight against cybercrime in the year 1997. It has established the "24 Hour Contacts for International High-Tech Crime" which has advanced its technologies to recommend ways to prevent cyber-crimes and countering terrorism. [18]
- "**Organisation for Economic Cooperation and Development- OECD":** Globalization has economic, social and environmental challenges which are addressed in the OECD. It has been adopting measures to secure the information systems as they found an importance in being the main component of globalisation. In 2002 they adopted special guidelines on "Security of Information Systems and Networks" to manage security planning and protection of information systems. This was an initiative towards controlling the menace of cyber terrorism and protecting the countries from its effects.

Not only OECD and G8, there has also been efforts from the Commonwealth Nations in taking a step towards protecting the world from cyber terrorism. It has created a model law for the nations to follow to protect their computer systems and to protect them from any kind of interference of data. [19]

[16] Talat Fatima, Cyber Crimes, 247 (2d ed. 2016).
[17] Nazura Manap, *Cyber Terrorism: Issues in Its Interpretation andEnforcement*, 2 INT. J. INF. ELECTRON. ENG. (2012).
[18] JODY R. WESTBY, *Countering Terrorism With Cyber Security*, 47 279–294 (2007).
[19] Manap, *supra* note 17.

REGIONAL ORGANISATION

Among the regional organisations, the ones who have contributed the most are the European Union and the Council of Europe. European Council was mostly responsible for the protection of human rights and the rampant attacks on the world occurring using the mode of cyber space opened its eyes towards the need of protecting and taking actions to safeguard the world against terrorism that occur in cyber terrorism. It invented " CODEXTER(Committee of Experts against Terrorism " which was to focus on cyber terrorism. Any illegal content or any kind of matter on the cyber space which encouraged terrorism was looked at and measures were taken to take that down. The "Convention on Cyber Crime" adopted by the Council of Europe became the first international treaty to curb the crimes committed on cyber space. A consistent international cooperation was the main objective behind its making.

Another organisation , " International Multilateral Partnership Against Cyber Terrorism (IMPACT)" found a lot of importance as it demanded a partnership between public and private governments in eradicating cyber terrorism. INTERPOL, UN, and International Telecommunication Union were the ones which supported its existence. Merging of domestic and international problems was the main objective. [20]

CONCLUSION

Globalisation has its own pros and cons. When one looks at the current scenario it becomes quite evident that globalisation has brought development in economic, technological, social, legal and political field . The nature of the computer world is dynamic and unstoppable. It has so many facets that a new one can be revealed every day. Globalisation has been dominated by US based countries or to be specific the developed countries creating a sense of resentment among the Islamic countries who have challenged their dominance by using methods of violence and aggression. The networking of such terrorists' groups is also something which is an outcome of globalisation. It uses of Information technology and cyber space has made them connect with each from the remotest of spaces. Looking at the current condition one can very out rightly say that probably terrorism or cyber terrorism is an outcome of globalisation and probably is in the way of

[20] *Id.*

becoming a global phenomenon. However when one sees the kind of international agreements and efforts made by nation to cope up with this growing menace it can also be predicted that probably only globalisation can be the method behind curbing the phenomenon of cyber terrorism.

THE CURIOUS CASE OF MODERN CYBER WARFARE: ISSUES AND CHALLENGES

Madhura Thombre-Kulkarni[1]

"*Science gathers knowledge faster than society gathers wisdom*"

-Isaac Amino

Abstract:

Technology is recognised as an enabler, necessary for growth and the way forward. Technological developments have touched every corner of our life and has provided us with countless opportunities. The recent decades have given rise to modern technologies of warfare which have led to unprecedented changes and means of conduction of the present warfare which has also led to an international disruption or change in power. Warfare technologies-once a part of science fiction, have become a reality and they have a potential to cause catastrophes. Cyber Warfare is one of the modern dimension of armed conflict capable of leapfrogging borders and bringing devastations of unimaginable magnitude[2]. The impact of cyber warfare on the civilian population can be considered is huge & diverse and the question as to whether the traditional rules governing the conduct of hostilities need to be applied or new rules must be re-formulated in case of cyber hostilities. Wars are becoming much more devastating and cyber warfare with its added advantage of low cost, deniability, anonymity and devastating impact on civilian population as well as on infrastructure, has raised grave concerns. The aim of this study is to study the growing weaponization of cyberspace in 21st century, elevation of cyber-attacks to a full-fledged cyber warfare and to check the viability of existing legal regime to address the legal and ethical concerns of cyber warfare.

Introduction

Cyber warfare has become a part of conflicts and the race of global power entering the fray of cyberwar is at its peak. Digital technologies have potential to exacerbate or change conflict dynamics and increase the risk of intentional and unintended harm to the affected population[3].

[1] Assistant Professor Navrachana University, Vadodara

[2] Andy Greenberg, *The WIRED Guide to Cyberwar*, WIRED (Aug 23, 2019) https://www.wired.com /story/cyberwar-guide/

[3] Delphine Van Solinge, *Digital risks for populations in armed conflict: Five key gaps the humanitarian sector should address,* HUMANITARIAN LAW & POLICY (Jun 12, 2019) https://blogs.icrc.org/law-andpolicy/2019/06/12/digital-risks-populations-armed-conflict-five-key-gaps-humanitarian-sector/.

The ever evolving nature of the cyber warfare in the present century has led to many challenges to the applicability of the laws. The main issue here is the changing nature of the state and non-state actors involved in these contemporary conflicts, difficulty in ascertaining the identity of attackers, asymmetrical nature of digital space and digital divide existing across the world. These issues are detrimental to the objectives of IHL and the present no-change and inefficient administration of the present international law has led to the only option i.e. justification and reflection of the present situations under the umbrella of IHL. Two categories of risks are noticed with increasing reliance on cyber operations in armed conflict:

1. Espionage or surveillance and use or misuse of the meta data for purposes intended to have humanitarian consequences.
2. Behaviour of practices that increase exposure to digital-related risks.

International Humanitarian Law (hereinafter referred as IHL) is generally associated with four ratified conventions of 1949 with Hague Convention, three additional protocols which give the three main principles of armed forces in combat i.e. Principles of distinction, proportionality and necessary precaution for minimal effect on citizens. IHL is basically the law that tries to govern the way in which warfare should be conducted, allowed weapons, rights of the combatants and finally, to protect the civilians who have been caught up in the war. IHL is more focused on how the war must be conducted between the parties rather than the reason of the war. Hence, when war actually takes place, IHL tries to moderate the evils of it by protecting civilians who are not involves at all as well as the weapons and methods which are incorporated in the war, as ultimately the aim of IHL is not to end war but regulate the conduct of parties during warfare. There is a need of relook at the humanitarian law principles in light of cyber warfare. The principles of state sovereignty and state responsibility under customary international law also need a relook in light of growing participation of non-state actors in carrying out cyber warfare.

Cyber Warfare:

With superior technological dimensions, wars are going to become much more devastating than earlier. Cyberwar and cyber warfare is one of such new dimensions of

conflict capable of leapfrogging borders and teleporting the chaos of war to civilians thousands of miles beyond its front[4].

Cyber warfare is a computer or network based conflict involving politically motivated attacks by one nation-state on the other or others. It is a conflict in virtual space waged via the internet to sabotage defence, financial or other computer systems by either nation –state or state sponsored entities. Distributed denial-of-service attack is increasingly being used for the purpose of cyberwarfare. Computer systems are being used as weapons and also as a target with an ultimate aim of espionage, infiltration, manipulation, disruption or even destruction of varying scale and magnitude. Most striking example of this decade is the Stuxnet malware attack on Iran's nuclear facilities damaging centrifuges of uranium enrichment along with several other industrial plants. This was alleged to have been masterminded by US and Israeli intelligence agencies to deter Iran from making advancements into the nuclear development programme. The problem was noticed only after the worm mutated itself to cripple hardware and consequently the equipment was set on self-destructive mode. This was probably the first time where a State used cyber weapons to sabotage the enemy.

The ubiquitous use of information technology as cyber weapons has already outstripped our ability to manage cyberspace safely. With advantages of deniability, anonymity and effectiveness; cyber weapons have already become a part of many states' armouries[5]. Successful attacks have opened a Pandora's box of troubles elevating the random cyber-attacks to the stage of state sponsored cyber warfare causing damages of unimaginable magnitude. In a world of heavy dependence on computer systems, deliberate sabotage against railway, airports, power supply grid, stock exchange, health system etc. causing virtual as well as physical damages has become a new weapon of war. Looking at the nature of attack, identity of the attacker and the targets- key infrastructures either physical or virtual, it is quite clear that the last decade has witnessed some of the worst forms of cyber warfare to which there is no stoppage. Russia is alleged to have been sponsoring several such denial of service attacks. The attack on Ukraine's election system to disrupt Presidential election in 2014 is a

[4]Andy Greenberg, *The WIRED Guide to Cyberwar*, WIRED (Aug 23, 2019) https://www.wired.com/story/cyberwar-guide/.
[5]THE NEWS, https://www.thenews.com.pk/magazine/money-matters/758044-the-foreseeable (last visited Dec 22, 2020).

leading example as to how cyber warfare can be used by States to sabotage enemies. Russian hackers attacked the computer system of

Bundestag- lower house of the German Parliament in 2015 and more recently in 2018-2021 with 'GhostWriter' cyber-attack. Defence and interior ministers, parliamentarians' private network are being affected and reports indicate a Russian hacker group Fancy Bar behind the attack[6]. Russia intruded the power supply companies leading to complete blackout in 2 lakh homes in Ukraine in 2016. It is a first known blackout in history carried by cyber-attack. This is a stark example of conflicts shifting to unconventional modes with the help of modern warfare technologies. China, North Korea, Iran have launched multiple cyber-attacks on critical entities in USA of various levels ranging from espionage to information warfare. The WannaCry ransomware alleged to have been released by North Korea did hit around 155 countries exploiting several flaws in Microsoft operating systems.

Now with COVID-19 pandemic, information technology has become an indispensable tool for almost all the sectors. It in fact has brought a magnified risk of cyber warfare leading to potentially disastrous consequences. Attacks on critical healthcare computer systems to bring health service delivery to a standstill, is no more a mere work of fiction. A massive ransomware attack on digital infrastructure of a hospital in Germany has allegedly led to delay in providing emergency care causing a few casualties. Several state-sponsored cyber-attacks have taken place on Pharmaceutical companies' vaccine database for commercial as well as political gains in 2020 and 2021.

US Energy department has confirmed a worst-ever cyber-attack has taken place on the critical infrastructure that hold USA's nuclear stockpile in December 2020[7]. Perpetrators have managed to breach the computer network and carried out espionage on range of key government departments of defence, homeland security, treasury etc. Timely detection of the massive attack probably has saved USA and the world from disastrous consequences but it is an alarming sign of an exacerbated threat that can lead to devastating consequences across the world. Series of attacks were detected on USA's vaccine research & development system.

[6] Cyber-attack on German Government is 'ongoing', https://www.bbc.com/news/world-europe-43248201 (Last visited on 25/05/2021)
[7] US cyber-attack, BBC, https://www.bbc.com/news/world-us-canada-55358332 (Last visited on 25/05/2021)

China and India are at loggerheads since the Galwan valley clashes in June 2020 and China is alleged to have been using hybrid warfare mechanism where the battles will be carried out in conventional as well as in unconventional manner through cyber warfare, information warfare, proxies & insurgencies and so on. Investigations are underway after a Cyber Security Agency 'Recorded Future' has reported a Chinese group 'RedEcho' backed by State to be behind the massive cyber-attack that paralyzed power supply system in its financial Capital-Mumbai and several other cities in India. A malware into power grid system has brought the commercial capital to a standstill for a few hours. Similar cyber-attack was attempted on the database of Indian vaccine manufacturing companies' database and investigations have indicated a potential link to Chinese state-backed agencies to be the culprits.

Cyberspace is being weaponized and the whole world is now a battlefield!

LEGAL AND ETHICAL CONCERNS:

Today, all our systems from traffic control to healthcare and from power supply to elections depend upon computer and network. Sitting at any corner of the world, any state or non-state agency can hack a computer system and practically paralyze a company, a city, a government and even a country. Politically motivated cyber-attacks itself is increasingly becoming a weapon of war due to its added advantages of anonymity, low-cost, asymmetry and consequences severe than the conventional armed conflicts. Seemingly inexorable ramp-up of the destructive potential of a cyber-war, the key question along with cyber-peace or cyber-security is, how about the applicability of Laws related to armed conflicts to these virtually waged acts of war?

New forms of contemporary warfare have given rise to several legal issues and the key question about applicability of laws remains a matter of great concern. It is perceived that International Humanitarian Law would not be applied in the present era of modern warfare. Every state and non-state actor is supposed to respect the existing norms of IHL rather than aiming for new rules. But such compliance, especially from non-state actors is a distant prospect.

State specific conflicts which are driven by international forces as well as unknown cyber forces. Extraterritorial military interventions and foreign military camps in other countries, cyber warfare, proliferation in intelligence communication through internet, rising

prevalence of non-state actors are some of the conflicts which need to be contained under IHL. IHL has been ratified by states which makes compliance by the non-state actors as difficult; these non-state actors practice asymmetric warfare in which IHL can be reinterpreted in such a way so as to suit their objectives. Russian backed cyber warfare against Ukraine is the best example to indicate the asymmetry.

The occurrence of contemporary cyber-warfare at places which have been closely connected with life of civilians makes it very hard to apply the principles of IHL. The presence of non-state actors which are sometimes not even recognised by the state as they feel that recognising them will give furtherance to their cause. International Law is commonly understood to be applicable to states and state agencies, international organizations. Growing participation of non-state actors which are tough even to be identified further complicates the applicability part.

The key question of applicability of principles of IHL has assumed greater attention. Citizens in technologically advanced countries with large scale internet penetration & reliance as well as citizens in places with comparatively lesser advanced countries are impacted by the strategic use of cyber technology for conflict purposes.

International Humanitarian Law seeks to regulate armed conflicts and protects civilians in wartime. In context of the changed periphery of nature of armed conflicts, it is important to determine what type of cyber-attack amounts to ‘warfare’ or rather an ‘armed attack’. Additional protocol to Geneva Convention of 1949 under Article 49 defines ‘attack’ means ‘all types of attacks’ and ‘the provision of the protocol with respect to attack shall apply to all types of attacks’. There is a general acceptance that when cyber operations destroy civilian or military assets or cause death/injuries to soldiers, civilians, IHL is applicable. It is less clear whether cyber operations that do not cause physical damage to civilian or military infrastructure or hostilities as per conventional understandings could be called as ‘resort to armed force by the State’ even though their impact is more devastating and consequently could IHL be made applicable to such operations or not! Ever evolving technology has expanded the arena of sophisticated cyber operations which could arguably be conducted outside the conventional understanding of ‘armed conflict’ leading to intended and unintended damages of unforeseeable magnitude. International Court of Justice in its advisory opinion on legality or threat of use of nuclear weapons emphasized that the

stablished principles and rules of IHL applicable in case of armed conflict shall apply to all forms of warfare and all forms of weapons including those of future[8]. There must be a common understanding of applicability of IHL Principles to cyber operations. Affirmation of principles should not encourage militarization of cyberspace or legitimize cyber warfare. While determining the applicability of rules, the interconnected nature of cyberspace and widespread incidental civilian harm must be duly considered[9].

Cyberspace offers a unique medium to nation-states to operate against a wide array of targets free from physical or geographical constraints. Nowadays, several states have acknowledged that they have been using cyber operations during armed conflicts and are investing into development of military cyber capabilities[10]. There is a general acceptance that, IHL and its principles are and shall be made applicable to conflicts waged in cyberspace. It has its own complexities and difficulties.

Due to interconnections in cyberspace, the effective regulation of cyber operations during armed conflict concerns all the states irrespective of the level of technological advancement[11]. Everything that has an interface with the internet can be affected by cyber operations conducted from any corner of the globe. Attack on one system will have repercussions on other connected systems. This interconnectivity of cyberspace practically means that all states irrespective of their location, tech-preparedness could be affected. In such cases, the 'digital divide' is a major constraint. States with lower technological advancement are more vulnerable than others. Their capabilities to detect, combat or even prevent a cyber-attack of warfare level is extremely limited and hence there needs a better clarity regarding applicability of IHL Principles to cyber warfare in an effective manner along with uniformity.

IHL applies to operations that are linked with armed conflict. When it comes to cyber-attack or even a cyber-warfare, attribution to a particular entity is very difficult. Attribution of cyber operations is extremely important to ensure that violators of international law and IHL

[8] ICJ, Legality of the threat of use of nuclear weapon (8th July 1996, Para. 86) .
[9]Laurent Gisel, Tilman Rodenhauser, *Cyber operations and international humanitarian law: five key points*, HUMANITARIAN LAW & POLICY (Nov 28, 2019)https://blogs.icrc.org/law-and-policy/2019/11/28/cyber-operations-ihl-five-key-points/.
[10]Id.
[11]Helen Durham, *Cyber operations during armed conflict: 7 essential law and policy questions*, HUMANITARIAN LAW & POLICY (Mar 26,2020)https://blogs.icrc.org/law-and-policy/2020/03/26/cyber-armed-conflict.

be held accountable[12]. For application of IHL principles, the attribution of attack to a State or state-sponsored entities is crucial. In a customary international law, for attributing any conduct to a State requires extensive evidence of a State backing or a control over the conducting entity. In a nutshell, definition of 'attack', 'armed conflict' under IHL need a relook along with the principles of state responsibility under international law in light of cyber warfare.

Another major concern of Cyber-warfare is that it has also triggered cyber arms race in the world and none of the cyber security initiatives have received much traction[13]. After a disastrous Stuxnet malware attack allegedly by US and Israel, Iran carried out Distributed denial of service attacks on banking systems in USA affecting the civilians. The roster of global powers entering the cyber warfare spray started growing. North Korea launched massive cyber-attacks against South Korea, USA and with WannaCry ransomware attack in 2017, it crippled the digital infrastructure of Chinese universities, Indian Police Departments, British National Healthcare system causing losses of around $4 to &8 billion. Russia used cyber warfare along with conventional warfare on Ukraine paralysing its power supply, transport system, banking systems etc. Global reluctance in coming together for cyber security or for limiting cyber arms race to limit threats of cyber warfare has actually given further impetus to state and non-state actors to employ cyber weapons as a part of state armoury.

Therefore, it is quite clear that cyber-operations as a means or a method of cyber warfare comes with a severe humanitarian cost. Cyber warfare has its own specific characteristics and there has to be a holistic review as to how the principles of International Law and International Humanitarian Law should be made applicable to this emerging form of warfare.

CONCLUSION

Due to the challenging developments, relevant concepts of 'State', provisions of State responsibility, state sovereignty under International Law and relevant concepts related to 'armed conflict' under International Humanitarian Law as well must be revised for a better reflection of the 21st century conflicts. IHL and war exist in a symbiotic relationship which changes and mould as the various situation in war changes which even addresses the new

[12]ICRC, *International humanitarian law and cyber operations during armed conflicts* (Nov 28, 2019) https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts.
[13]

changes and asymmetrical warfare.[14]Issues which have been created due to the contemporary warfare have actually led to the decreasing relevance of IHL. Many have said that IHL has become an archaic law and amendments need to be introduced but, even though IHL does not reflect the realities of the contemporary warfare but they can still be applied in practice. Active participation of non-state actors which are not even recognised or are working with proxy identities in conflict makes accountability extremely difficult. There should be an increased awareness of the incentives and benefits that would be given to non-state actors to enhance the principle of reciprocity between state and non-state actors. Information warfare is an integral element of cyber warfare. Civilian objects are duly protected against attacks under International Humanitarian Law. However, there are differing opinions as to whether data enjoys the same protection under IHL in the event of attacks targeting the data. There should be a holistic review of the legal principles in context of heavy reliance on data in the rapidly digitizing world. Also, global powers must arrive at a consensus for a comprehensive cyberspace regulation and a mechanism to prohibit growing weaponization of the cyber space. There must be an independent and permanent international entity to address concerns arising out of contemporary cyber warfare & cyber-attacks so as to ensure a responsible behaviour from States and subjects in the interconnected cyberspace. The global digital divide and consequent asymmetry must also be addressed in order to effectively implement cyberspace regulations.

[14]Michael N. Schmitt, *Asymmetrical Warfare and International Humanitarian Law*, 11GEORGE C. MARSHALL EUROPEAN CENTER FOR SECURITY STUDIES, GARMISCH-PARTENKIRCHEN.

SOCIAL MEDIA AND THE EMERGING DIMENSIONS OF CYBERCRIME IN INDIA

Bharti Sharma[1]

Abstract

Social media is a mode of interaction and communication, but the hitch in social media involves many more things rather than just meeting new people. Technology plays an important role in our life with many advantages there is a list of disadvantages that adversely affect human life. During Covid-19 period life without Internet would be like fish out of water. In this pandemic, not just our work or studies but everything even our relations, shopping, bank instalments and many more depends on social media and internet. Internet acted as an instrument in the development of technology therefore it is by no frivolous means to suggest that Internet has made interaction and communication so easy and has made a profound contribution in the development of technology throughout the world. With so many ongoing activities offences relating to cheating by personation, defamation, identity fraud, cyber bullying, phishing, cyber terrorism, obscenity and many more can be easily performed with the help of social media and internet. The reason of so many crimes is lack of awareness among people and authorities lack behind in technology. Obscurity over Internet and jurisdiction issues also lead to many cyber crimes. This research paper aimed to apply doctrinal legal research method for cyber crime analysis and provide a critical review of the literature on this topic and focus on all legislative and judicial approaches regarding cyber crimes, case laws, obligations of State and judicial trends.

Literature Review

The review of literature is of immense importance as while writing a research paper the main focus is to develop a new argument. In a research paper, literature is used as a support for new vision. The purpose of literature review is to make a summary of ideas and arguments of others in order to get some recommendations for present research work.

The future is still up for grabs between criminals and normal users. a brief survey post and to assess the rate of cyber crimes showing an alarming high number of businesses facing frauds. Internet is proving itself is effective despite of the criminal activities. (N.Tapaswini & D.Summanjit "Impact of cyber crime issues and challenges", 2013) Not only

[1] Student UPES Dehradun

coming but commercial entities producing software's also can play an important role in stopping fraud.

(P.Rekha "Impact of social networking on cyber crimes", 2018) All the facts and circumstances prevailing in the country was assessed and it can be stated that there is a need to bring changes in IT act to combat cyber crime and proper technology should be adopted

The impact of cyberspace on society is undeniable. Cyber attacks and online threats are surfacing Internet. (B.Maria & N.Jason "The social and psychological impact of cyberattacks", 2019) it is important to see the psychological and social impact of cyber attacks.

Empirical study showed that out of 100 respondents majority believed the social media has a negative impact. WhatsApp was the most famous social media network followed by YouTube Facebook and Internet. (H.Sajeesh, S.Archana & P.Nehajaon "Study on effect of social networking sites on the Young world of cybercrime", 2018) Watch on all the sites that children are using and awareness should be spread among children.

While examining the threat of cyber crimes the alleged factors such as reasons that lead to rise of cyber crimes, penance mechanism and traceable techniques of cybercriminals has not been taken into consideration.

Introduction

Internet has greatly affected our lives, With the advancement of technology it is also fair to say that criminal activities have also increased. Attackers who are experts in technology by using the tools and mechanisms of Internet are easily able to commit crimes on line. Web pages are designed in such a way that they can invade privacy of people and are so interactive that people easily get prey to frauds through these social networking websites. As nowadays during this pandemic people are using Internet for net banking, paying bills, shopping because of these facilities a lot of network security issues evolved. Cybercriminals can easily hack these social media platforms and through social media these malware practices are carried out by attackers. They know the weakness of people and also they never fear of getting caught. This paper deals with the subject of relation between social media and cyber crimes and aims to take abroad sweeping look at social media platforms and cyber crimes.

First the links between social media and cyber crimes are discussed, the second part mark off the case evidence and the methodology of study and the third part presents the findings A concluding precise ends the paper.

Meaning of Cyber Crime

Cyber crimes involve computer oriented crimes and crimes through modern technological networks. Cyber crimes are high profile crimes and are committed to cause fraud, identify theft and privacy violation. Traces of cyber crime can be found in US. Americans were the first sufferer and sinners of cyber crime. By 21st century in the whole world cyber crimes were spread. Attacks through cyber crimes do not effect physically but they effect mentally and virtually. Cyber crime is a very wide term and it is difficult to define it in one or two sentences. Cyber crime is active globally and is developing at a very rapid rate and it's very dangerous as the identity of the offender is difficult to identify.

Historical Background of Cybercrime

In 1970[2] when first version of Internet was introduced security was not an issue as people do not have access to Internet but it is a matter of time when that door was exploited. In 1971 a message "I am the creeper catch me if you can" created several users of the APRNET, this computer worm was made with no malicious intent but pave the way often for vulnerabilities that explored Internet. In 1989 the first record of denial of service attack in history occurred. Robert Morris created a worm that dramatically slow down Internet speed this worm was not created with any malicious intent but to show the flaws of security but disaster occurred when a fault in its code caused it to replicate excessively causing extensive damage and partition of the entire Internet that lasted four days that same year was the first ransomware attack although poorly designed and easily removed the aids Trojan was created by Joseph Popp to extort money this malware was distributed in floppy disk by regular door to door. Luckily one short day an act was passed in UK that made any unauthorised use of computer system illegal this act not only brought cyber security to forefront it became the foundation of cyber security protection. 1995 was the birth year of SSL. The secure socket layer is an Internet Protocol that encrypts communications between computing device and online destination. The SSL 2.0 version that was released in 1995 was a bedrock for the hypertext transfer protocol secure more commonly known as https which often is at the

[2] Retrieved from https://www.floridatechonline.com/blog/information-technology/a-brief-history-of-cyber-crime/ on 27-11-2020

beginning of web addresses when browsing securely. With the release of windows 98 in 1999, cyber security along with everyday casual computing effectively went mainstream the massive spike in computer use with this operating system paved the way for a host of security software. Windows released a series of patches to improve protection of software while the production of anti hacking software for home computer were blossomed in 2000. With over 10,000,000 windows user were infected with the i love you bug the fastest breeding worm in computer history at that time this pervasive email sentence attachment when opened activated a worm this worm overruled random files and sent a copy of itself to every address within outlook. In 2002 the US Department of Homeland security, designated groups to protect IT infrastructure which today has evolved into a large division dedicated to cyber security then anonymous was born the first infamous group of hackers known to the world this group has a vast network of users with no leader often acting in interest of protecting the privacy of the everyday person one of their more notorious digital heist was the hacking of the Church of Scientology website with their now in famous grey Fawkes masks steadily in place. 2010 saw the strike of operation Aurora, this was the year Google announced a coordinated breach of its infrastructure in China their whole purpose was to unmask intelligence operators of US law enforcement agency watch list. In 2013 Yahoo fell victim to one of largest scale hacks in industry when over 3 billion user accounts were compromised by installing malware directly on Yahoo, hackers gained virtually unlimited backdoor access revealing a wide host of confidential user information all that can be seen as a crescendo to probably the most infamous security breach of all time. In 2016 wiki leaks hackers from the Russian intelligence agency published private documents from Democratic committee emails this entire affair dramatically affected how Americans viewed that years election becoming a sobering example of how cyber crime could influence international politics. Cyber crime is not defined under Indian law but a legislation has been introduced to tackle it. The first cyber crime of India was Yahoo Inc versus Akash Arora[3] in this case the defendant Akash Arora adopted the domain name Yahoo india.com The Honourable court held that Yahoo word has distinctiveness and thus belongs to plaintiff and injunction was granted to defendant restraining him from using the mark Yahoo.

Social Networking Websites

[3] Yahoo Inc v Akash Arora (1999 PTC (19) 201 Delhi)

Social media are interactive websites through which users can communicate online and can share their content, also through social media users can interact with each other and now social media is used by people for business marketing too. There are 376.1 million users of social networks in India. Most popular social networking sites in India are Facebook, WhatsApp, Instagram, LinkedIn and Twitter.

Historical Background of Social Media

From 1997 to 2000[4] the social media website ever created was called 6 degrees by using 6 degrees people could socialise and communicate with anyone who created a profile. During the same time a man named Justin Hall was busy creating the first blog website, this service allowed the social media world to take a huge jump forward its the thought of blogging websites that let people to find new ways to communicate via the virtual world this led to creation and use of instant messages services derived from the English phrase ICQ, the Israeli company ICQ became insanely popular at that time. AOI then bought ICQ in the 2000s and improved its services making instant messaging one of the ways of human communication this allowed people to communicate about more things more often and at anytime that was more convenient for them. The easiest and fastest way to get a date at that time was through the Internet. In 2003 a website called LinkedIn was launched. LinkedIn allowed job users to post their CVS and employers to post job offerings this contributed greatly to the diversity of Internet and is an ongoing service until today. In the same year the Golden age of the social networking site Myspace was born. Myspace dominated the social media world removing Google from the top of the list of the most visited websites in US in June 2006. Myspace died out and was basically replaced by the current social media site Facebook starting from a Harvard dorm in 2004 Mark Zuckerberg[5] and his roommate created what would be the world's most popular and most visited social media website in the world what used to be a network for Harvard University students has now more than a million users worldwide today. Facebook greatly influence significant aspects of daily life such as music, art, business and politics it's also worth mentioning that Facebook was called the Facebook in its beginnings before Sean Parker the inventor of Napster advised Mark Zuckerberg to change its name to what we now know today as just Facebook. A year later lieu de corp a Vancouver based company created Flickr a site that focuses on photo sharing inspired by Flickr, Jack Dorsey and his colleagues invented Twitter. In 2005 Flickr was bought by

[4] Retrieved from https://www.google.com/amp/s/www.convinceandconvert.com/social-media-strategy/how-social-media-has-evolved/amp/ on 29-11-2020

[5] Retrieved from https://vamp-brands.com/blog/2020/02/28/evolution-of-social-media/ on 30-11-2020.

Yahoo. Yahoo also bought the infamous Tumblr two years later. In 2012 Twitter bought the company Vine and owned over 50 other social media companies. The more recent and popular photo sharing platform Instagram was founded in 2010 in San Francisco. Snapchat was created by three Stanford University students in 2011 this image messaging system has now incorporated features such as calling video chatting and texting. These are just some of the major social media platforms available for any computer or mobile device other platform such as Attack and ask FM was also a huge hit since they allow users to give their opinion in an anonymous way. Similarly other platforms like Tinder allow users to meet new people in real life, Reedit and Pinterest are similar to Flickr and Tumblr. There are literally thousands of other social media platforms that are available nationwide and globally.

Categories of cybercrime

- Cyber terrorism : Cyber terrorism is any planned activity in the cyberspace via Internet or computer to create terror in the social space. It is an act of using cyber technology to threaten the security, unity and supremacy of the nation.
- Cyber stalking : Active frequently revisiting a web page or social profile of organisation or individual.
- Child pornography: Act of exploiting child right by online video streaming containing illegal content.
- Cyber theft: Cyber theft is stealing confidential information or private data.
- Cyber trespass: It is a form of sniffing data in a computer system without actually altering or deleting it.
- Cyber fraud: Active selling fake items on Internet by gaining trust.
- Cracking: A malicious act of breaking into a computer or a computer network with wrong intentions for tampering with the information.
- Hacking: Hacking is a process of exploitation of a computer system to gain access.

There are three categories of hackers[6] white hackers, grey hackers and black hackers.

White hackers: They work to keep data safe from other hackers by finding and fixing security loopholes, they offer their services to corporations, educational institutions to make the network more secure.

Black hackers: Hackers with criminal intentions. They are motivated by personal gains like to steal confidential information and to crack bank accounts for money stealing.

[6] Retrieved from https://www.designworldonline.com/what-are-the-three-types-of-hackers/ on 1-12-2020

Grey hackers: They include those who hack for fun or to troll. They do not do it for personal financial gains. They are associated with black hackers.

- Phishing: It is an attempt to acquire sensitive personal information like passwords, credit card details from people through fake means.
- Cyber bullying: Cyber bullying aims at blackmailing or shaming the victim basically its a type of harassment that is done through digital means.
- Cybersquatting: It is the practise of registering names especially well known company or brand names as Internet domains to play the sellers and earn profits.
- Pornography: It is an act of exchanging, exhibiting and trading obscene contents with pictures and videos.
- Debit and credit card fraud: A debit or credit fraud is where a person steals the credentials of a person debit or credit card to do unauthorised payments or take cash out from the account of a person.
- Denial of service attack: A denial of service attack is when attacker shutdown some network depriving the users to use that site. Denial of service attack creates traffic in the site which cause the server to buffer and then slowing it down to stop. Denial of service attacks usually happens on banking, media, government, commerce trade sites. It leads to wastage of time and money to handle the attack.
- Fake profiles on social media: Scammers with the help of fake profiles on social media targets legitimate profiles for distribution of malware, offensive content, fake service and coupons for seeking money and information.
- Catfishing: It is the best example of fake profiles on social media, profile is created with the intent of seducing the victim for extortion of money.
- IPL violations: IPR violations is infringement of patent, copyright and trademark. In social media usually people try to copy the content of others thus causing financial loss to a person by doing counterfeits and piracy.
- Ecommerce frauds: Ecommerce frauds is when a fraudster do business with the merchant using stolen or fake credit cards for transactions thus leaving the merchant with no payments.
- Email spoofing: Email Spoofing is forgery of the senders address to mislead the recipient about believing that email originated from intended source but in reality it originated from somewhere else.

- Email bombing: It is a method in which large amount of emails are sent to the victim resulting in the crash of victims email account or server.

Case Studies

Cyber Attacks

1. Cosmos Bank Malware Attack

   In 2018 cosmos Bank of Pune faced a cyber attack, 94 crore rupees were transferred illegally from cosmos bank account. The bank claimed that no customer bank accounts were affected. The attack was executed for about 2 hours 13 minutes from about total of 21 countries with total of 12,000 transactions, this was a very well planned act of robbery done by persons even one person was identified from Hong Kong. Several switching systems were put in place and there were dummy cards used to do these transactions. 2.5 crores remained in the accounts, 450 cards were used for transactions. In India itself 2800 cards were used, in Canada first transaction was done.

2. Canara Bank ATM Hacked

   In 2018 The ATM servers of Canara Bank were hacked. Cyber attackers had details of 300 users using the skimming method and got information of debit cards of people. ₹20,00,000 were efface from the accounts of people. 10,000 to 40,000 transactions were done.

3. UIDAI Aadhar Card Software Hacked

   In 2018 the data of 1.1 billion people holding Aadhar card was leaked. From 210 government websites data of people was leaked and was being sold on Whatsapp in ₹500.

4. Indian Healthcare websites hacked

   In 2019 according to US cyber security firms Indian healthcare websites were hacked and thus data of 68 Lac patients and doctors was stolen.

5. SIM Swap Scam

   In 2018 two hackers transferred four crore rupees from bank accounts of several people. They gained SIM card information fraudently and by using fake documents through online banking transactions were done by them.

6. Bengaluru Hospital Bank Account Hacked

   Bank account of Bengaluru hospital was targeted and ₹17,00,000 was stolen through cloning the SIM cards.

7. Wipro phishing attack

   A phishing attack was done on Wipro through gift cards thus compromising the accounts of various employees and clients of Wipro.

Data Breach Cases

1. Twitter

   130 Twitter accounts were targeted in July 2020 by phone spear-phishing method. By targeting the employee credentials attackers were able to get the access to the internal system and were able to download 36 inbox chats and data of seven accounts.

2. Zoom Credentials

   In April, 2020 five lacs zoom accounts were hacked by credential stuffing attack and were sold for free or for just a penny on dark web.

3. Unacademy

   In January 2020 the US firm pointed out that 20,000,000 user accounts of Unacademy were hacked their usernames, password, details of login, email and names all were sold on dark web.

4. Big basket

   In October 2020, 20 million users of Big Basket faced data breach as their personal details were being sold on sale of $40,000 on dark web.

5. Nintendo

   In April 2020 three lacs ID account of Nintendo were compromised. The accounts were breached where certain users were contacted directly and while others passwords were reset.

6. Marriott

   In January 2020,5.2 million guest of Marriott faced data breach not only their personal information was breached but also their details like birthday month, gender, partnership and company details were also exposed.

Social Media Cases

1. Umesh Kumar Sharma v State of Uttarakhand & another[7]

[7] Retrieved from https://indiankanoon.org/doc/112614373/ on 5-12-2020

Umesh Kumar Sharma uploaded a video on social media in which certain documents were shown, the screenshot of certain bank accounts that showed that bribe was taken by the CM of Uttarakhand as money was transferred to the accounts of his relatives. High Court ordered CBI probe into allegations of corruption however Supreme Court had stayed the High Court order of filing FIR against CM.

2. Marico limited v Abhijeet Bhansali[8]

   Abhijeet Bhansali, a social media influencer in his YouTube video claimed that Marico parachute coconut oil is not 100% pure and he was promoting products that are in competition with the parachute oil. Court observation was that social media influencers have a great effect on people and that they should apply caution and shouldn't post such content that is harmful or offensive and the video that was posted by Bhansali was injuncted from being displaying on YouTube.

3. Me too Movement

   In October 2018 me too movement on Twitter started in India. Women came out with their stories of sexual harassment, rape and misconduct and named their abusers. Tanushree Dutta accused actor Nana partaker of sexual harassment and then there was a series of posts by other woman from actors, director's, artist, politicians, journalist all were named in the me too movement. However in India there were defamation cases filed against women who were not able to prove allegations but the Sexual Harassment of women at workplace (Prevention, Prohibition and Redressal) Act 2013 was strengthened.

4. Bois locker room

   A group of boy teenagers in a group chat on Snapchat use to send objectionable pictures of girls and used abusive language for girls and talk about gang raping them. On 2 May 2020 A Instagram user spoke about how she got screenshots from someone who was a member of that group. FIR was registered by the police. A journalist on Twitter told that a minor girl used fake identity of a minor boy name Siddharth to see the reaction of the receiver boys. Although police said that no action will be taken against the girl as she is a juvenile and it is a childish act.

5. Baba ka dhaba case

   YouTuber Gaurav Wasan shot a video of Kanta Prasad and his wife famously known as Baba ka dhaba in South Delhi telling that the couple is having lack of customers

[8] Retrieved from https://indiankanoon.org/doc/112614373/ on 5-12-2020

and is facing financial issues thus many people donated money for them. Prasad told that he received a cheque of 2 lacs rupees from Wasan. In the cheating complaint filed by Prasad, he told that Wasan deliberately shared his bank account details and collected donations. Other you tubers alleged that Wasan received 20-25 lacs however Wasan showed his bank account details and after the complaint gave three lacs rupees more to Baba.

6. Chinese Apps ban

   In June 2020, Ministry of electronics and IT of India banned 267 apps of China as they were threat to sovereignty and integrity of India and were trying to collect information and causing personal security breach.

7. IRCTC hacked

   A software developer from Jharkhand used an illegal software to generate tickets by hacking the railway website. Mustafa who hacked the website had 563 IRCTC ID's and had 2400 accounts in SBI and 600 accounts in regional rural banks. The RPF has arrested him he was a follower of the Pakistan religious group and is generating money for terror attacks.

8. Twitter account of PM hacked

   The Twitter account of PM Narendra Modi was hacked, a tweet was posted that asked followers to donate to PM National Relief Fund through cryptocurrency. John Wick was behind the hack. Later Twitter administration confirmed that account was hacked and they are investigating and the tweet was also taken down.

Legislations dealing with cybercrimes

Throughout the world cyber security agencies are working for the prevention of cyber crimes. Similarly in India apart from IT Act 2000 and 2008, Indian Penal Code, Copyright Act, Companies Act, Terrorism Act and IT Act 2011 were adopted to address the offences committed through Computer and Internet, from petty fines to life imprisonment are awarded as a punishment in these offences.

Offence	Trail under Sections	Punishment
Hacking	Section 43A and 66 of IT Act 2008 and Section 379 and 406 of IPC	3 Years Imprisonment or ₹5 lacs fine

Data Stealing	Section 43B,66-E,77-C of IT Act 2008, Section 379,405,420 of IPC and Copyright Act	3 Years Imprisonment or ₹2 lacs fine
Cyber war or terrorism	Section 66f of IT Act 2008	Life Imprisonment or fine
Identity theft	Section 43,66C of IT Act 2008 and Section 419 of IPC	3 Years Imprisonment or ₹1 lacs fine
Email Spoofing and fraud	Section 77B of IT Act 2000,Section66D of IT Act 2008 and Section 417,419,420,465 of IPC	3 Years Imprisonment or fine
Pornography	Section 66A of IT Act 2008 and Section 292,293,294,500,506,509 of IPC	On first conviction: 5 Years Imprisonment or ₹10 lacs fine On second conviction: 7 Years Imprisonment
Child Pornography	Section 66B of IT Act 2009, Section 292,293,294,500,506,509 of IPC	On first conviction: 5 Years Imprisonment or ₹10 lacs fine On second conviction: 7 Years Imprisonment or ₹10 lacs fine
Debit or Credit Card Fraud	Section 66C of IT Act 2008	3 Years Imprisonment or ₹1 lac fine
Denial of service attack	Section 43(e),(f) and(g) of IT Act 2008	Compensation

Conclusion

During COVID-19 crisis cyber crimes has increased immensely and India is among the least cyber secure countries in the world the reason for increase in cyber crime is unemployment and people being experts in computer can commit these crimes easily as conviction in cyber crime cases is quite low in India. Although Government has taken steps to deal with cyber crimes like Ministerial committee on phone fraud, national cyber crimes

reporting portal is launched by central government, also personal data protection bill is made and it will be passed by the Government of India in upcoming years. Still there is a need to bring adequate changes in IT act also, cyber crime is spreading at an uncontrollable rate on social media as fake websites and accounts are not blocked by government officials and no adequate steps are taken by police immediately thus more people fall prey to these cyber crimes even after they are reported. There is a need to spread awareness about cyber crimes among people that how they can browse safely and should handle their social media handles. It can be concluded that in upcoming years there is a presumption that Internet will be a definite part of our life as it is today so it is important to secure Internet and traceable techniques of cybercriminals needs to be upgraded.

SUBHRANSHU ROUT @ GUGUL V. STATE OF ODISHA – AN INSIGHT INTO THE RIGHT TO BE FORGOTTEN AS A FUNDAMENTAL RIGHT IN THE CYBER REALM

Sanjana Kulkarni[1] , Shrirang Ashtaputre [2]

ABSTRACT:

Since time immemorial, mankind has been keen on recording information and passing it on from one generation to another as a matter of legacy – religions, customs and rituals have found their way into the modern society owing to the ability of our ancestors to preserve such data. In fact, this was considered as a matter of duty and carrying forward the legacy of our ancestors, even today, is considered as a matter of pride. In this Information Age, practically everything is largely dependent on data, including one's identity, which, on falling in the public domain, becomes difficult to be altered or even changed. Owing to great technological development, information is largely stored in the cyberspace and reaches the corners of the world in few seconds, deleting which, is certainly not an easy task. Although the scope for editing one's identity certainly exists in India, whether one can completely erase the data of himself/herself from the society is still being contemplated in our Constitutional Democracy. Known as the right to be forgotten, a notion borrowed from foreign jurisprudences and heavily pondered upon by the Supreme Court in **K.S. Puttaswamy v. Union of India**, Indians do have, as of today, the right to be left alone. And recently, the High Court of Odisha, in **Subhranshu Rout @ Gugul v. State of Odisha**, sought to expand upon this notion by asserting the need to direct the social media private platforms to be able to delete objectionable information of individuals for protecting their dignity. Enlightening the masses about the nuances of this verdict, the Authors, through the medium of this paper shall also elaborate upon the development of the right to be forgotten in both foreign and Indian jurisdictions and determine the understanding of the term "objectionable content" in the light of this right. Besides, the Authors shall examine whether the private social media entities are indulged in performing any public duty within the meaning of Article 12 for making them accountable for truly enabling the implementation of the aforesaid right in the cyber-realm which is truly the need of the hour.

[1] Student V B.A.LL.B, ILS Law College, Pune; Email:sanjanakulkarnilaw12@gmail.com
[2] Name: V B.A.LL.B, ILS Law College, Pune: Email: sr.ashtaputre@gmail.com

INTRODUCTION:

One of the interesting facets of the humankind is its ability to label every particular entity or an event for ensuring their survival, thereby giving a true purpose to mere existence – in the words of Devdutt Pattanaik, humans, after all, cannot fathom living in a meaningless world with actually no task to perform! The ardent need for identifying however is believed to be a crucial reason for several atrocities committed against people for centuries together – for instance, the patriarchs, by associating themselves to be superior to all other humans, claimed primacy over all other genders and consequently, framed and utilized laws for curbing the freedom of latter social groups, such as women. The British and later the Americans and the South Africans sought to distinguish people based on their colour for exploiting other races and exploiting them for personal gains. Merely on the basis of skin complexions, these countries evolved segregation laws and even today, are a serious cause for hate crimes committed against the Black population in the United States of America. Even in India, the members of the Dalit and the Shudra fraternity were and unfortunately in some parts of India, are mistreated owing to their surnames, a label bestowed by the priestly classes of the ancient subcontinent. After all, it was caste which helped in determining the status of a particular individual in the society and was cleverly utilized by the British to assert control over Indians. Koreans can never forget the aggressive measures undertaken by Japanese empire during the early 20th century for wiping out the native culture and replacing it with that of the latter, in terms of festivals, traditions, administration etc[3]. Neither can the residents of Maharashtra disregard the efforts of Muslim sultanates to wipe out the religious identity of Hindus herein – Chhatrapati Shivaji Maharaj rebelled against the Mughals in the hopes of preserving the same[4]. Where these civilizations fought extensively for preserving identities, scholars like Dr Ambedkar on the other hand, worked tirelessly in reforming the society by giving the oppressed classes a new identity[5] – post-independence not only did the members take up the surnames utilized by the upper classes but many converted to Buddhism, in the hopes of creating a better and a safer future for themselves and their generations to come. The aspirations of the freedom fighters and the political circles for the

[3] South Korea and Japan's feud explained BBC News Dec 2, 2019. As retrieved from: (https://www.bbc.com/news/world-asia-49330531).

[4] YED ALI NADEEM REZAVI Why Shivaji broke away from the Mughals — and established the Maratha reign Daily O Apr 12 2018. As retrieved from: (https://www.dailyo.in/variety/shivaji-empire-mughals-treaty-aurangzeb-agra-mughals/story/1/23418.html).

[5]SIDDHARTH Why Ambedkar chose Buddhism over Hinduism, Islam, Christianity The Print May 20 2019 1:08 pm IST As retrieved from: (https://theprint.in/opinion/why-ambedkar-chose-buddhism-over-hinduism-islam-christianity/237599/).

Indian society, void of all forms of social classifications are well-reflected within Article 14 of the Constitution of India[6], 1950 which asserts equality and equal opportunity before the law and its Article 17[7] and Article 18[8] which avers the need to do away with untouchability and discard the usage of all forms of titles in the country respectively. It would be safe to assume that constant efforts appear to have been undertaken by the State for extinguishing all forms of social identities to eliminate any form of oppression in the future – although these social evils have seeped into our modern democracy, social integration does appear to have been achieved in the country. Nevertheless, on reading it with Article 21 of the Constitution of India, 1950[9], it is evident that every individual has the freedom to be perceived the way he or she wishes to and that any form of racial or casteist slur would be equivalent to crushing their dignity and therefore, a punishable act. And where India recognizes the freedom of privacy including within its ambit, the right to identity of choice and that of self-expression, the State can hardly interfere in the said matter, unless, it is against the general welfare of the masses. And while its creation and maintenance are largely encouraged by law, its anti-thesis, i.e., the right to be forgotten largely goes unnoticed and in fact, needs to be discussed and elaborated upon in the light of several technological changes that have transpired over the last few decades.

RIGHT TO BE FORGOTTEN – AN OUTLOOK:

The right to be forgotten, i.e., the erasure of certain data of a person at his or her choice, appears to correspond significantly with the idea of the State to forgo all forms of identities which may hinder in its quest of creating a peaceful society. The said concept owes its origins to the desperate need for people to remove their memories from the cyberspace, a hub, where dozens of images, videos and data are uploaded and circulated every second. Due to the growing reliance upon social media websites for connecting with citizens, finding suitable job opportunities etc, the world has become self-conscious with regards to the way they are discerned and people often resort to refining the how they seek to be recognized in the society. Naturally, one might find it difficult to cope up with any particular data pertaining to them which they do not approve of being exposed in the cyberspace and this is precisely why, upon the demand of the user, the removal of such data is justified. Realizing

[6] Constitution of India, 1950, Article 14 – Equality before Law.
[7] Constitution of India, 1950, Article 17- Abolition of Untouchability.
[8] Constitution of India, 1950, Article 18- Abolition of titles.
[9] Constitution of India, 1950, Article 21- Protection of life and personal liberty.

the need for permitting its individuals to revamp their identity as per their convenience, the European Union, through its General Data Protection Regulation sought to enforce the right to be forgotten within its jurisdiction by directing the controlling authority to completely erase the certain data upon the request of the subject. As per Article 17, one can successfully get the data erased after:

- lack of necessity of retention of data,
- withdrawal of consent as per the provisions of the Regulation,
- objection by the data subject with lack of overriding grounds to such objection,
- unlawful processing of such data and the need for erasure owing to legal compliance[10]

Unlike Europe, it is unclear as to whether a particular individual can direct the State to erase particular information relating to him or her from the data unless it is obscene or defamatory. While this ignorance breaches the right to privacy of the individual, any action with this regard would amount to infringing the freedom of speech and expressions of the citizens as envisaged in Article 19(1)(a) of the Constitution of India, 1950[11]. Reading this with the impact of the verdict laid down in Justice ***K.S.Puttaswamy(Retd) v. Union Of India*** [12], the fundamental right to be forgotten, a subset of the right to privacy should, supersedes the general freedoms of the citizenry. After all, society has no right to interfere, deliberate and comment upon the personal choices of individuals, unless it concerns the best interests of the State or affects them directly. This suggests that in the Indian context, the right to be forgotten is an objective privilege and is rather provided to the citizens for enabling the State to maintain order in the society – this is precisely why the executive authorities, upon appeal by the citizens for removing sexually explicit/unwarranted/ calumnious content from the internet is bound to undertake the same. Rather, this privilege adds teeth to the Information and Technology Act, 2008 for satisfying its purpose of eradicating the misuse of internet and protects the essential rights of the citizens therein. To put it simply, the scope of the right to be forgotten is limited and to date, nearly all the judgments rendered by the Indian judiciary with this regard involve a narrow interpretation. Undoubtedly, its application does fail to extend to cases where the said content has been uploaded on the private social media

[10] Right to Erasure, Article 17 of the GDPR. European Parliament and Council of European Union (2016) Regulation (EU) 2016/679.
[11]Constitution of India, 1950, Article 19(1)(a)- All citizens shall have the right. (a) to freedom of speech and expression.
[12] (2017) 10 SCC 1.

platform, such as Facebook! A similar scenario was witnessed in ***Subhranshu Rout @ Gugul v. the State of Odisha***[13], wherein the Court opined:

"In fact, the information in the public domain is like toothpaste, once it is out of the tube one can't get it back in and once the information is in the public domain it will never go away."[14]

The said case rightly brings forward the aspects of horizontal application of fundamental rights and ascertaining the scope of the aforesaid right and at the same time, examining the position of the revered social media platform, Facebook as "State" within Article 12 of the Constitution[15], compelling the Authors to discuss the said order:

Subhranshu Rout @ Gugul v. the State of Odisha – An Insight

It is undisputed that teenagers and young adults have greater exposure to sexually explicit materials and owing to the drastic changes in lifestyle and other external factors, tend to mature earlier in comparison to the trend of the yesteryears. And it is through these technologically advanced gadgets that these individuals make connections with persons of their sexual preferences and try exploring each other by engaging in relationships – in no time, they tend to indulge themselves in sexual activities and it comes as a surprise that the same is regretted by many. What adds on to this grief is the mysterious desire for recording these private movements, which, several times, is used by either partner, mostly the males, for securing favours from the other participant – its failure is usually met with the circulation or the uploading the images/videos on social media platforms or other websites. In such situations, approaching the Police becomes a tougher job as revealing such personal information to the officers becomes difficult for the individuals and a matter of shame for the family - considering the orthodox society, it comes as no surprise its members tend to disassociate the female victim herself! Importantly, even if the State were to take cognizance and direct the removal of such lewd content from the cyberspace, there is no guarantee of the same ever happening and it would continue to persist and be accessible to millions, safely placed in its deep corners. What is unfortunate, despite being aware of such misuse, humans often fail to realize the consequences of such acts and its impact on their lives and future, as witnessed in this case above – though unlike other precedents of similar nature, the High Court of Odisha, while rejecting the plea for bail in the aforesaid matter, demanded the

[13] BLAPL No.4592 OF 2020.
[14] Id.
[15] Constitution of India, 1950, Article 12 – State.

execution of the right to privacy and hence, that of being forgotten against the Facebook for getting the images and the videos removed at the earliest.

Facts:

Petitioner Rupali Amanta was immensely in love with the accused and they had an affair for one year and on the last day of Kartik Puja, the accused gruesomely raped her and recorded the said incident and threatened her to publish the same in the public domain if she confided about the same. Upon her narrating the incident to her parents, the accused uploaded the same in the cyberspace, where after she lodged an FIR against him. Charges were brought under Sections 376, 292, 465, 469, 509 of the Indian Penal Code, 1860 read with Sections 66, 66(C), 67, 67(A) of the Information and Technology Act, 2008 and amidst the pendency of the proceedings, an application for regular bail was made, whereby it was urged to release the accused as he had an ITI Diploma and staying behind bars would only hinder with his prospects of securing a job. Furthermore, the Counsel on behalf of the accused promised to marry the victim informant. The State, on the other hand, reiterated the forced sexual intercourse, repeated on further occasions under the warning of being exposed to the world in unpleasantly. The subsequent disclosure of intimate scenes of the female victim was deemed as a crime of serious nature by the Counsel, who reminded the Court of the unbearable trauma faced by the victim at the hands of the accused.

Judgment:

Quite commendably, the learned Judge heavily read through the judgments rendered by numerous foreign and Indian jurisdictions with regards to the scope and implementation of the right to be forgotten for analyzing the extent to which the same can be exercised for removing images etc. so uploaded on Facebook herein. While rejecting the application for regular bail, the Court suggested the victim and the prosecution seek orders for protecting her privacy and to have the said content removed from the public platform at the earliest.

CONSTITUTIONAL OBLIGATION OF FACEBOOK TO SAFEGUARD THE RIGHT TO BE FORGOTTEN IN INDIA:

At the outset, the Authors appreciate the stance of the Court for rightfully making out a case for revenge porn, so understood as sharing of sexually coloured images, videos etc.

without the consent of the person involved in the same[16], and on that basis, rejecting the plea for the Bail – in a way, this significantly helps in shaping the discretionary power of the judiciary with regards to dealing with and curbing such illegal activities which are not declared as offences in the country. This stance confirms to the stance of the Allahabad High Court and the Bombay High Court, which have rejected applications for Bail in matters involving blackmailing the victim of leaking the obscene recordings[17] and for uploading such pictures of the victim in the cyberspace without her consent respectively[18]. Revenge porn usually manifests when an unauthorized person, releases intimate photographs, videos etc. thereby exposing their sexual parts of the other person extending to sexual penetration of allied activities without his or her consent, amounts to revenge porn[19]. It may involve posting sexualized pictures of either of the partners or ex-mates on public forums to gather sympathy and demean them brutally[20]. In either case, the primary goal is to cause immense emotional distress to the other person. Although revenge porn is not explicitly an offence in India, the fact, a person blackmailing and subsequently posting obscene pictures of women or any other person for that matter on public platforms in India can be held guilty of 354C (Voyeurism), 354D (Stalking) and 509 (Criminal Intimidation) of the Indian Penal Code, 1860 read with sections 66C (Identity theft), 66E (Violation of privacy) and 67/67A (Transmitting obscene material online) of the Information Technology Act 200[21]8. Be it noted that any form of extortion is a violation of the right to personal liberty of the individual besides the fact that the women possess the right against rape and that against sexual harassment is recognized by the Constitution, expecting abidance from both Government and private individuals.

With regards to the liability of private entities for not infringing with the dignity of the individuals, a plethora of verdicts of the Indian judiciary help us conclude that they could be amenable to writ jurisdiction under Article 32 of the Constitution[22], provided it is sufficiently proved that they were exercising public duty or were engaged in a business which catered to or affected the best interests of the citizens therein. State can act through an agency or an instrumentality and a public authority within the meaning of Article 12 of the Constitution of

[16] Revenge Porn – What it means for the victim and the offender Safeline. As retrieved from: (https://www.safeline.org.uk/revenge-porn-what-it-means-for-the-victim-and-the-offender/).
[17] *Veena Verma v. State Of U.P. & Another* CRIMINAL MISC. BAIL CANCELLATION APPLICATION No. - 18501 of 2009.
[18] *Akshay Sripad Rao v. The State of Maharashtra* CrBA 2304/17.
[19] N.J. STAT. ANN. § 2C:14-9(c) (West 2013).
[20] *Fighting Cybercrime After United States v. Jones* 103 J.CRIM. L. & CRIMINOLOGY 745, 794 (2013).
[21] *State of West Bengal v. Animesh Boxi* Case no:- GR: 1587/17.
[22] Constitution of India, 1950, Article 32 - Right to Constitutional Remedies.

India, 1950 and can make profits for the public benefit[23]. If the function of a particular private body is greatly related to the function of the State, then, other factors, such as Governmental aid for running it become immaterial and such a corporation then falls within the ambit of Article 12 of the Constitution[24]. It is established that the concept of instrumentality or agency of the State extends to organizations created by statute and those which exercise public duty or function on the monies provided by the Government[25]. The need to expand the horizon of Article 12 of the Constitution is imperative to discipline entities for sheltering the rights of individuals in the country[26] - the misuse of Facebook by individuals certainly calls for better a mechanism to curb the same.

Notably, Facebook is bound to remove illicit content which is likely to affect the unity, integrity and sovereignty vide the India Information and Technology (Intermediary Guidelines), Rules, 2011 - this suggests that it is considerably controlled by the Government. These Rules demand the removal of such content which is in a nutshell, is defamatory and obscene and violates the very dignity of the person[27]. The Court has the power to direct the removal of such data from these websites globally and the respective Public Policy Head is expected to ensure compliance with the same besides the aforesaid regulations, further indicative of the influence of the state. Despite having such power, it is surprising as to why the Court, while deciding upon the Bail did not suggest the removal of the said content which degraded the victim in the first place.

It must be borne in mind the onset of Facebook in India radicalized the freedom of speech and expression herein, providing people with an ideal platform for engaging in discussions and deliberations, which, is an ideal characteristic of a prosperous State. On several occasions, the Apex Court has pointed out the exchange of information is an integral facet for ensuring the well-being of the masses[28] since the free and general discussion on public matters is essential for the sustenance of democracy[29]. With changing times and the growing needs of the society, there is a need for the Government to meet the demands of the citizenry and reliance to that effect was expected to be placed on private bodies for ensuring

[23] *Rajasthan State Electricity Board v. Mohan Lal* 1967 SCR (3) 377.
[24] *Sukhdev Singh v. Bhagat Ram* AIR 1975 SC 1331.
[25] *P.M. Machaiah v. Mysore Sugar Co. Ltd*. 1963 SCR (2) 976.
[26] *M.C. Mehta v. Union of India* 1987 SCR (1) 819.
[27] *Swami Ramdev & Anr. v. Facebook, Inc. & Ors.* CS (OS) 27/2019.
[28] *Dinesh Trivedi, M.P. and Ors v. Union of India* 1997 (3) CLT 21.
[29] *Maneka Gandhi v. Union of India* 1978 AIR 597 1978 SCR.

their happiness[30]. In simple words, Facebook and its other social media setups such as Whatsapp and Instagram have aided the Government in promoting the right to speech and expression and ensuring the holistic development of the citizens, thereby contributing majorly to the development of the welfare state – initially, it was due to Facebook that families staying abroad could connect easily and cheaply, businesses could reach out to a greater number of clients, peaceful gatherings or protests manifested, travelling became convenient and importantly, dialogues on issues pertaining to governance became easier. Such has been the importance of Facebook and other social media handles, which run on the internet in the cyberspace that the Supreme Court, in ***Anuradha Bhasin v. Union of India***[31], declared the right to the internet as a fundamental right within Article 19 and Article 21 of the Constitution for free speech and the right to carry out occupations of choice, which later, was extended by the High Court of Kerala to include the right to education[32]. It would not be wrong to say that Facebook enabled the modernization of the Indian society by enabling it to connect with the residents of a developed nation and exchange views, opinions, knowledge and learning! These developments and indistinguishable nature of the functioning of Facebook and the duty of the State to ensure welfare as per Article 38[33] compel the Authors to conclude Facebook as State[34] within the meaning of Article 12 of the Constitution[3536].

Besides the positive impact upon Indians also, these technological facilities are vulnerable to misuse by miscreants who have attempted to influence the citizenry in a negative way, even infringing upon the dignity of others on numerous instances– one cannot forget the misleading post by the nephew of MLA, Akhanda Srinivasa Murthy who was

[30] *Ramana v. International Airport Authority of India*1979 AIR 1628.
[31] 2020 SCC OnLine SC 25.
[32] *Faheema Shirin.R.K v. State Of Kerala* 2019(2) KHC 220.
[33] Constitution of India, 1950, Article 38 - State to secure a social order for the promotion of welfare of the people.
[34] Although the Authors have attempted to bring Facebook within the ambit of Article 12, it is agreed that the State does not have deep control, or as affirmed in *Pradeep Kumar Biswas v. Indian Institute of Chemical Biology & Ors.,* (2002) 5 SCC 111, administrative, financial or economic control over it. Moreover, mere regulations of the State over the private entity by the Government does not render it as State and therefore, the Authors have also discussed the aspects of horizontal-application of Fundamental Rights therein.
[35] Although the Directive Principles of State Policies, so envisaged in Part IV of the Constitution of India, 1950 cannot be enforced, the Judicial Forums of India, on numerous instances, have permitted its application for strengthening the implementation of fundamental rights herein. See *Ashoka Kumar Thakur v Union of India* (2008) 6 SCC 1, *Subhash kumar v. State of Bihar* AIR 1991 SC 420, *Mohd. Hanif Quareshi & Others v. The State Of Bihar*1959 SCR 629, *Har Shankar v. Deputy E. and T. Commr*,1975 SCR (3) 254.
[36] A particular organization is undertaking a public function, such as the one by Facebook makes it amenable to writ jurisdiction within the confines of Article 226 of the Constitution. See *BCCI v. Cricket Association of Bihar and Ors.*(2015) 3 SCC 251.

responsible for communal riots in Bengaluru[37]. At the same time, the spread of fake news and rumour through the medium of these platforms largely goes unnoticed despite the redressal mechanism and is likely to bring about disharmony in the society[38]. With regards to the present case at hand, the stature and the privacy of people can be violated by uploading their pictures without prior permission and yet, administrative action with this regards to the removal of such content is sluggish. This naturally calls for the arising need for holding Facebook, a private entity liable for failing to take adequate measure to prohibit the aforesaid activities. One way of doing this is reaffirming the principles of horizontal application of fundamental rights, i.e., binding private entities to shelter and respect the fundamental rights of other citizens therein. In simple words, the verdict rendered by the Court in ***K.S. Puttaswamy Case***[39] does pave the path for implementing and the same in matters about safeguarding the very dignity of the individuals. However, the development of this jurisprudence has continued to manifest since the 1980s – in ***People's Union for Democratic Rights and Others v. Union of India and Others***[40], it was asserted that Article 17, 23[41] and 24[42] of the Constitution of India could be enforced against private individuals as well. This was precisely why the Apex Court penalized firework industries when they were found guilty of employing children in hazardous activities[43]. In ***M.C. Mehta v. Union of India***[44], the private entity so responsible for the oleum gas leak in Delhi was directed to compensate the individuals and deaths and injuries for depriving them of their lives/causing injuries illegally. A similar scenario was observed in the Bhopal Gas Leak Case, whereby, under the pretext of the principle of Absolute Liability, the private organization was yet again made to redress the damages caused to the citizenry[45]. In ***M.C. Mehta v. Union of India***[46], where the Ganga, source of water to the residents of Kanpur, was being polluted by the tanneries, the Supreme Court placed the best interests of the individuals above the right of a few to carry out the business of choice and directed to halt such exercise at the earliest. A similar case was

[37] Aditi Phadnis Offensive Facebook post leads to riots in Bengaluru, three dead Business Standard Aug 12, 2020 23:27 IST. As retrieved from:(https://www.business-standard.com/article/politics/offensive-facebook-post-leads-to-riots-in-bengaluru-three-dead-120081201775_1.html).
[38] *Alakh Alok Srivastava v. Union Of India* 2020 SCC OnLine SC 345.
[39] Supra 10.
[40] (1982) 3 SCC 235.
[41] Constitution of India, 1950, Article 23- Prohibition of traffic in human beings and forced labour.
[42] Constitution of India, 1950, Article 24- Prohibition of employment of children in factories, etc.
[43] 1991 SCC (1) 283.
[44] Supra 24.
[45] (1989) 2 SCC 540.
[46] 1988 AIR 1115.

witnessed in ***Vellore Citizens Welfare Forum v. Union of India***[47], wherein the Supreme Court, on noticing grave pollution of river Palar which could affect the lives of those using its water, imposed a fine on the tanneries. Replicating position appears to have been undertaken by the said Court in ***Vishakha v. State of Rajasthan***[48], whereby the Court, besides administering the averments of the international obligations within the municipal laws, declare sexual harassment by any individual as a violation of the right to dignity of women within Article 21 of the Constitution – in ***Bodhisattva Gautama v. Subhra Chakraborty***[49], rape was declared as an abrogation of the bodily integrity of females. These cases provide abundant material to suggest that private entities such as Facebook could be held guilty for failing to remove proscribed information from its area of operation and for harbouring those resorting to such illegal means, even by the citizens. Suffice to say, that the said jurisprudence can be outstretched for effectively enforcing the right to be forgotten in India; although a few judicial forums have had the opportunity of scrutinizing such cases and propounding verdicts, which have rendered a narrow interpretation of the right[50]. The right to erasure can be averred to arise from the right to be left alone with protection against unwarranted interference of the society in personal matters, such as choices, sexual orientation etc[51]. Consequently, the names of the rape victims and such offences are expected to be kept confidential[52] and the right to be forgotten could also be applied for protecting persons from baseless allegations so as to safeguard their personal and professional interests[53]. It is mischief if any accusations made in defamatory contents are published without any legal sanction[54]. Unlike India, Turkey has recognized the right to privacy to be inclusive of the right of the individual to control his or her past broadening to securing the removal of such data pertaining to previous penalizations or such photos which damage their reputation[55]. Even in the United States of America, where publication of such incidents of the pat-life of a person without his or her consent, which are likely ridicule him/ her was deemed as a violation of the right to privacy[56]. However, such a liberal outlook does not prevail in

[47] 1996 5 SCR 241.
[48] AIR 1997 SC 3011.
[49] (1996) 1 SCC 490.
[50] *Dharamraj Bhanushankar Dave v. State of Gujarat* 2017 SCC OnLine Guj 2493.
[51] *R. Rajagopal v. State of Tamil Nadu* 1994 SCC (6) 632.
[52] *Nipun Saxena v. Union of India* (2019) 13 SCC 715.
[53] *Zulfiqar Ahman Khan v. Quintillion Business Media Pvt. Ltd. and Ors.* 2019 SCC OnLine Del 8494.
[54] *Subodh Gupta v. Herdsceneand* 2019 SCC OnLine Del 11209.
[55] Turkey: The Supreme Court Decision on the Right to be Forgotten Mondaq Nov 12 2019. As retrieved from: (https://www.mondaq.com/advicecentre/content/3110/The-Supreme-Court-Decision-on-the-Right-to-be-Forgotten).
[56] *Melvin v. Reid,* 2016 Hu No. 45.

India at the moment and has been pointed out by the Supreme Court in ***K.S. Puttaswamy Case***[57], wherein it refused to permit a wider interpretation of the said privilege in India to the optimum, as envisaged by the Western Nations and the GDPR. That is to say, that the averments of the European Court of Justice with regards to the enforcement of the right to be forgotten to the extent of permitting erasure of any data of choice, cannot be implemented in India as a whole – in doing so, this forum did impose a limitation for exercising this freedom by refusing such request when it is justified by the "*preponderant interest of the general public*"[58]. In simple words, there may be instances when a person may be, irrespective of his or her willingness, be required to emerge from seclusion in the best interest of the public and in such cases, the claim of right to privacy would not be justified[59]. This is precisely why, the data controller is vested with the discretion of deleting information in the cyberspace and he or she may reject the same, upon weighing the demand of the individual with the freedom of speech and expression of the general public[60] – even the Data Protection Bill, 2018[61] provides for a similar approach with regards to implementing the right to erasure in India. In times where the Supreme Court of India asserts for the implementation of Constitutional Morality[62], avoiding the free exercise of the right to erasure is clearly in violation of the right to privacy itself[63]. Nevertheless, prohibiting the violation of this right with regards to the matter at hand stipulates that Facebook, in either case, is bound to remove such lewd content, which tends to violate the dignity of the citizen (the victim herein) unlawfully.

CONCLUSION:

The Authors opine that for safeguarding the right to privacy of the individuals, their needs to exist a right to erasure in the first place and ignoring this facet *prima facie* leads to the violation of the former right. There indeed, is a dire need to elaborate upon its scope to cope with the prevailing international standards with regards to civil and political rights of global citizens. Where the Central Government is seeking to enforce stricter measures against platforms such as Twitter so as to assert maximum control over its activities under the pretext

[57] Supra 10.
[58] *Google Spain SL & another v. Agencia Espanola de Protection de Datos* Case C-131/12.
[59] *Jones v. Herald Post Co.* 18 S.W.2d 972.
[60] *Google LLC v. National Commission on Informatics and Liberty* Case C-507/17.
[61] Personal Data Protection Bill, 2018, Section 27 - Right to Be Forgotten.
[62] *Navtej Singh Johar v. Union of India* (2018) 10 SCC 1.
[63] Undoubtedly, the Authors are not bidding for an absolute implementation of this right and information which truly concerns the masses should not be erased is accepted. Unless the data pertaining to an individual impacts the society, the intervention of the latter with that regard is unjustified.

of "national interests"[64], the Authors plead for declaring "revenge porn" as an offence and devise a better mechanism for removal of such content, for protecting the dignity and well-being of women and other individuals in such situations. It is high time that the concerned authorities accept that sexual violence could also extend to damage to the bodily integrity of citizens even in the cyberspace and take its cognizance at the earliest. Undoubtedly, recording and posting any images or videos of any person without the consent of the concerned person indeed amounts to a blatant violation of their fundamental rights and yet, rapists and sadists operate this way on daily basis, obliviously and fearlessly – this indicates the amount of respect rendered by the common man to the Indian law, also conveying the minuscule value and the immense hatred against women in their minds. This rightly calls for the need to make people aware of their rights and limitations with this regard, which shall truly enable the State to halt the growing number of rape cases against women in India (at least in the cyberspace), which indeed is the need of the hour.

[64] Anuj Srivas Understanding the Nuances to Twitter's Standoff With the Modi Government The Wire Feb 12 2021. As retrieved from: (https://thewire.in/tech/twitter-modi-government-block-section-69-a).

CENSORSHIP ON INTERMEDIARIES: A SOLUTION TO STOP MISUSE OF SOCIAL MEDIA?

Dr. Kavita Goel[1]

Abstract

Internet intermediaries are kind of service providers providing services online. And while performing functions, may act as an information carrier or information publisher or information seller or online interactive board through World Wide Web. This may include social media like Facebook.com, Orkut.com, Youtube.com and Twitter.com etc. The boundary between information publisher and information seller is fast blurring as the rapid advance of e-commerce is transforming the publishers into sellers of services and products as well. Then the question arises what would be the liability of such publishers who are doing E-commerce as well? Sec 79 provides the balance between technology necessity and legal necessity over the liability of social networking websites. Now after The Information Technology Amendment Act, 2008, they are not liable for third party information or communication made available on their website. Before this amendment in Information Technology Act, 2000, in Bazee.com case, intermediary was exempted from liability because of lack of knowledge of selling obscene video on Bazee.com. According to The Information Technology (Intermediaries Guidelines) Rules, 2011, intermediary has to disable the objectionable content within 36 hours of take down notice and the storage of same for 90 days for investigative purposes. Proposed amendments to intermediaries' liabilities focus on akvitacaution on Misuse of Social Media and spreading Fake News. The rules water down the 'safe harbor Rule' for Intermediaries and force them to screen the content and exercise self-regulatory online censorship. And the process of blocking website containing doubtful content by social media is going against constitutional safeguards of natural justice and fundamental rights.

INTRODUCTION:

When the computers were invented, it was used first as a messaging system, something like a quick telegram or for making quick computation like a calculator. Slowly, it came to be used as a mean for e-commerce and advertising. We cannot deny the fact that the kind of life we are enjoying today, became possible because of such technology. It has

[1] Dr. Kavita Goel**,** Assistant Professor, Baroda School of Legal Studies, Faculty of law, The Maharaja Sayajirao University of Baroda

improved our lives, and now things are better, faster, easier and more convenient. It effects the way we communicate, learn or think. In this global pandemic situation; online schools, online offices, online supply of basic essentials, online medical consultancy, online communication with friends and family could be possible because of this technique. But all these, we can enjoy only if intermediary does their duty honestly and without bias and also look after the privacy of the users. Because dependency is increasing on the services of intermediaries and millions of people are creating their presence in virtual space.

Social Networking Sites and its Impact

The big wave of social networking sites has hit almost every corner of the world in cyberspace. In India, 84 percent users visit social networking sites which makes India the World's seventh largest social networking visitor. Currently the biggest social networking channel Facebook has around 700 million subscribers across the globe. While there weren't even a billion people using social media back in 2010, the number exceeded more than 2 billion within just five years. In 2019, there were around 2.77 billion people using social media.

These platforms impart a positive impact as it allows people to share their views with their distant friends and relatives within few seconds. It has also negated the effects of geographical distances in our social lives as one can make friends on these sites without knowing each other physically. And now internet has grown up to exercise one's right to freedom of speech and expression, a Fundamental Right protected under art 19 of Constitution of India. But many people fail to understand when free speech can take a form of hate speech, defamatory, offensive, menacing, insulting, annoying, politically or religiously sensitive, against public morality or decency or likely to create public disharmony. The right to privacy is also becoming a major concern because Facebook and other networks require user to register their mobile numbers apart from name and e-mail address for registration and activation of user accounts. Therefore, a lot of personal information is shared with an intermediary like social networks that ought to keep such information safe as per sec 43 A of Information Technology Act, 2000. WhatsApp's new policy has recently received criticism due to concerns over a potential increase in data sharing with its parent company Facebook.

Social Media as Intermediary

An intermediary means any person who on behalf of another person receives stores or transmits the record or provides any service with respect to that record. The Information Technology Amendment Act, 2008, has given an inclusive definition of 'Intermediary' under sec 2(1) (w) of Information Technology Act, 2000. It identified asset of service providers whether professional or non-professional as 'intermediary' like telecom service providers, network service providers, internet service providers, web hosting service providers, online payment sites, search engines, online auction sites, online market places, interactive websites and cyber cafes. Here interactive websites includes Facebook, Twitter, BlogSpot and Instagram etc.

Intermediaries may be broadly classified as information carrier, information publishers or information sellers depending on their functional attributes. It may also happen that the information publisher is not only publishing its own content but also buys from other content providers or third parties or third parties are allowed to upload their own content on the platform provided by such websites like social media websites like facebook.com, Orkut.com, Youtube.com, Twitter.com etc. in the context of internet, the boundary between information publisher and information seller is fast blurring as the increasing prospects of e-commerce is moulding the publisher into seller of services and products as well.
Then the question arises what would be the liability of such publishers who are doing E-commerce as well? It is important to note that Central Government has notified the Information Technology (Intermediary Guidelines) Rules 2011 for the purpose of creating due diligence practices to be observed by these intermediaries.

Liability of Intermediaries

Intermediaries represent technological innovation, which can be used in a lawful manner or unlawful manner. It was thus felt by the lawmakers that any provision, which would limit the role of intermediaries might affect the growth of internet, therefore the balance was needed. Sec 79 of Information technology Act, 2000 provides that balance between technology necessity and legal necessity. Sec 79 clearly exempted the intermediary from the liability for any third party information or data made available by him if he could prove that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent commission of such offence or contravention under original Information Technology Act, 2000. In Avinash Bajaj V. State, an obscene MMS video was listed for sale on Bazee.com and Supreme Court of India held that Avinash Bajaj,

Managaing Director of website, is not liable for the company's actions and he could not be implicated under the provisions of IT Act for the company was not arraigned as an accused in the case. Following this case, amendments in sec 79 were brought about to provide immunity to all intermediaries in connection with content made available from the third party. In this amended section, the burden of proof is no longer with the intermediaries and it is for the prosecution to establish the liability of an intermediary.

It means social media websites are not liable for the defamatory or illegal or prohibited content posted by third party if theses websites observed due diligence and guidelines of Central Government while discharging their duties under Information Technology Act, 2000.

'Due Diligence' that is to be observed by intermediary is given in Information Technology (Intermediary Guidelines) Rules 2011 which includes

a. The intermediary shall publish the rules and regulations, privacy policy and user agreement for access-or usage of the intermediary's computer resource by any person.

b. The intermediary through such rules shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that

i. belongs to another person
ii. is grossly harmful, harassing, blasphemous defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever;
iii. harm minors in any way;
iv. infringes any patent, trademark, copyright or other proprietary rights; (e) violates any law for the time being in force;
v. deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature;
vi. impersonate another person
vii. contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource;
viii. threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting any other nation

c. The intermediary shall not knowingly host or publish any information or shall not initiate the transmission, select the receiver of transmission, and select or modify the information contained in the transmission as specified above

d. The intermediary, on whose computer system the information is stored or hosted or published, upon obtaining knowledge by itself or been brought to actual knowledge by an affected person in writing or through email signed with electronic signature about any such information as mentioned in sub-rule (2) above, shall act within thirty six hours and where applicable, work with user or owner of such information to disable such information. Further the intermediary shall preserve such information and associated records for at least ninety days for investigation purposes.

e. The Intermediary shall inform its users that in case of non-compliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer resource, the Intermediary has the right to immediately terminate the access or usage rights of the users to the computer resource of Intermediary.

f. The intermediary shall adopt reasonable security practices and procedures as prescribed in the Information Technology (Reasonable security practices and procedures and sensitive personal Information) Rules, 2011.

g. The intermediary shall publish on its website the name of the Grievance Officer and his contact details as well as mechanism by which users or any victim who suffers as a result of access or usage of computer resource by any person can notify their complaints against such access or usage of computer resource of the intermediary or other matters pertaining to the computer resources made available by it. The Grievance Officer shall redress the complaints within one month from the date of receipt of complaint.

Censorship of Social Media Content

Recently, the issue of pre-censor of the third party information posted on social media networking websites like Facebook, Twitter and Instagram came into highlight. The Information technology Rules, direct the social website to monitor the content existed on their website and required them to take off illegal content within 36 hours from actual notice or knowledge of the content.

Section 69A of the Information Technology Act, 2000 empowers Government to block any information generated, transmitted, received, stored or hosted in any computer resource: (i) in the interest of sovereignty and integrity of India, (ii) defence of India, (iii)

security of the State, (iv) friendly relations with foreign states, (v) public order or (vi) for preventing incitement to the commission of any cognizable offence relating to above.

Year-wise detail of no. of URLs blocked on social media platforms are as follows:

Year	No. of URLs ordered for blocking
2016	633
2017	1385
2018	2799
2019	3433(till 31st October 2019)

Indian government has introduced a draft policy of rules that are intended to curb the misuse of social media and stop spreading of fake news. Under the new draft rules, all “intermediaries” are required to “proactively” purge their platforms of "unlawful" content or else potentially face criminal or civil liability. The rules also require services to make information about the senders of content and messages available to government agencies for surveillance purposes. This is a sharp blow to end-to-end encryption technologies, used to secure most popular messaging apps like whatsapp.

In an advisory issued by Ministry of Electronic and Information Technology on 20th March 2020 to curb false news or misinformation on corona virus, social websites were directed to initiate the awareness campaign for their users not to upload or circulate false information concerning corona virus which are likely to create panic among public. Social media platforms are urged to take action to disable or remove such content from their websites.

Social Media is intended to be a place where people shall be free to express themselves and share opinion with others in cyber space. But the arbitrary provision of taking down content without giving opportunity to creator of the content runs contrary to Freedom of Speech and expression.

In 2015, in the landmark Shreya Singhal judgement, the Supreme Court for the first time recognized the Indian citizen’s free speech rights over the Internet by striking down the draconian Section 66A of the IT Act. Further, regarding intermediary liability, the Court held that “Section 79 is valid subject to Section 79(3) (b) being read down to mean that an intermediary upon receiving actual knowledge from a court order or on being notified by the

appropriate government or its agency that unlawful acts relatable to Article 19(2) are going to be committed then fails to expeditiously remove or disable access to such material…. "it would be very difficult for intermediaries like Google, Facebook etc. to act when millions of requests are made and the intermediary is then to judge as to which of such requests are legitimate and which are not."

In Kamlesh Vaswani V. Union of India, The Supreme Court issued directions to intermediaries to disable specific content where website operating child pornography was sought to be restricted. In My Space Inc. V. Super Cassettes Industries Ltd., the court held that the Intermediaries can be held liable if they have actual or specific knowledge of the existence of infringing content on their website from content owners and despite such notice, they do not takedown the content. In Kent Ro Systems Ltd & Anr vs Amit Kotak & Ors, the Court held that "to hold that an intermediary, before posting any information on its computer resources is required to satisfy itself that the same does not infringe the intellectual property rights of any person, would amount to converting the intermediary into a body to determine whether there is any infringement of intellectual property rights or not… The IT Rules, according to me do not oblige the intermediary to, of its own, screen all information being hosted on its portal for infringement of the rights of all those persons who have at any point of time complained to the intermediary… Merely because intermediary has been obliged under the IT Rules to remove the infringing content on receipt of complaint cannot be read as vesting in the intermediary suo motu powers to detect and refuse hosting of infringing contents… I am of the view that to require an intermediary to do such screening would be an unreasonable interference with the rights of the intermediary to carry on its business." Thus, the Court reiterated the specific knowledge principle of the Myspace case.

Liability of Social Media in other Countries

The US Congress enacted Communications Decency Act in 1996, not to treat providers of interactive computer services like other information providers such as newspaper, magazines or television and radio stations, all of which may be held liable for publishing or distributing obscene or defamatory material. It opted not to hold interactive computer services liable for their failure to edit withhold or restrict access to offensive material disseminated through their medium. Title II of the Communication Act of 1996 was amended by adding sec 230 which provides that no provider or user of an interactive

computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

In the United Kingdom, it was held by Eady J., that an internet service provioder which performed no more than a passive role in facilitating postings on the interent could not be deemed to be a publisher at Common Law. It was essential to demonstrate a degree of awareness in order to impose legal liability for publication of words.

The European Commission's Directive dated June 8, 2000 is consistent with the Sec 230 of the Communication Decency Act, 1996. The Internet service provider is not liable as long as it acts as a mere conduit of information provided by others and they are not liable if the provider did not have actual knowledge of illegal activity or information and provider upon obtaining such knowledge acted expeditiously to remove or to disable access to the information.

As the internet and related technologies are spreading, the intermediary liability is decreasing the world over. But it is the time to put some restriction on their freedom.

Censor by Social Media

US President Donald Trump had lost his most important mean of communication when Twitter shut down Trump's account permanently where he shared his thoughts with 90 million followers almost daily, even hourly. Facebook and Instagram also indefinitely suspended his account. The social websites being, private Companies should not be making decisions on curbs to freedom of expression. According to US election watchdog group named 'Thomas More Society's Amistad Project' in the US, Facebook CEO Mark Zukerberg and his wife spent 500 million dollars in recent US elections favouring one political party over another. In Dec 2020, Russia announced that it could ban Facebook, Twitter, You tube for censoring content based on complaints from the Russian citizens. Poland passed the bill slapping $ 2.2 million fine for even a single message censored. The UK and European Union are setting strict rules with massive fines for these social media companies. European Union proposed two bills, one on illegal content and another on anticompetitive behaviour that could empower regulators to levy fines up to 10% of annual worldwide revenue on social media giants. These uncontrolled social giant have captive audience of population and has power to manipulate the voter's mind in any democracies. India has a need to balance

between freedom of expression and censoring anti national content. By dominating online access to political news, information, and discussion, Big Tech exercises an inordinate amount of influence over public opinion. Politically-motivated censorship online, therefore, advantages certain political interests and promotes certain views to the detriment of others, moulding public opinion according to particular narratives.

Through monopoly power, Big Tech gains an almost unfathomable degree of control over what information the public consumes. To combat Big Tech's censorship, the breaking up of monopolies through new antitrust legislation and proper regulation is essential. As companies such as Facebook, Whatsapp and Google are effectively conglomerates. Now they are not playing the role of intermediary but the controller of content of their platform where opinion of the users and readers are restricted.

FROM TEST TUBE BABIES TO HUMAN CLONES: EXPLORING RED BIOTECHNOLOGY FROM THE LENSES OF LAW

Paridhi Dave[1], Himanshu Bhargava[2]

Abstract

In the contemporary era, biotechnology has emerged as a promising venture for propelling the development and implementation of technological applications across diverse sectors such as healthcare, environmental conservation, energy and food security. 'Red' biotechnology is a branch of modern biotechnology, wherein the techniques are utilized in the field of healthcare, pharmacology or medicine. Red biotechnology has a significant role to play in the production of human cells, diagnostic of the gene and gene therapy. Tracing the journey to the past few decades, progress is noticed in various areas ranging from reproduction techniques such as *in-vitro fertilization* (IVF) to the production of human stem cells.

While biotechnology offers potential advances in the healthcare sector, certain concerns have been raised over time about possible irreversible modifications to the extant human gene pool. Pressing questions such as protection of human subjects in clinical trials, privacy, affordability and bioterrorism form part of the ethical concerns that have been brought forward.

In this paper, the authors attempt to explore red biotechnology, covering aspects such as reproductive medicine, advanced biomedical therapies, using human embryos for research, and human cloning. Further, these aforementioned areas shall be explored from the lenses of law and policy, at the domestic and international level. Since the production and usage of human cells and all forms of cloning have caused controversies across the globe, this paper shall also examine the bioethical dilemmas that arise from the innovation and utilization of these novel technologies.

[1] 3rd Year, B.A. LL.B. (Hons.) student at the Institute of Law, Nirma University, Ahmedabad. daveparidhi07@gmail.com.

[2] 3rd Year, B.COM LL.B. (Hons.) student at the Institute of Law, Nirma University, Ahmedabad. hbhimanshu.23@gmail.com.

PART – I: INTRODUCTION

Karl Ereky, a Hungarian scientist devised the term "biotechnology" in 1919.[3] This field of biotechnology has arisen out of the wider branch of biology which postulates the utilization of the biological systems, living organisms and cutting-edge technology to produce useful products having multifarious applications, namely in the field of agriculture, healthcare, food security, environmental conservation and security among others. The spurt of biotechnology in the global mainstream research and development in the last three decades has been instrumental in driving the pace of growth.[4] This has been largely possible because of the development of state-of-art technology to develop, map and manipulate existing genetic codes of the organisms.

Biotechnology is a vast field of research and it has been divided into various sub-fields for compartmentalization convenience. One of the major sub-fields of biotechnology is red biotechnology which deals with human healthcare by utilizing veterinary products.[5] This field has become a *sine qua non* to medicine in the 21st century which is predominantly used for gene therapy, clinical research and trials, diagnostics, regenerative therapies, development of vaccines and medicines, IVF technique, tissue engineering and production of biochips among other uses.[6]

India is a leader in biotechnology industries across the globe.[7] Red Biotechnology shares about 64% of the 63 billion dollars biotechnology industry in India.[8] This sector has been growing at a rapid speed of 16% every year leading the pack among other core sectors. Therefore, Red biotechnology holds a significant place in India due to its financial and social impact. In a neo-conservative country like India, the use of red biotechnology for reproductive, cloning and regenerative therapies holds a lot of ethical and legal implications.

[3] Der-Chin Horng, 'International Law On Biotechnology'
[4] 'What is biotechnology?' (*NTNU*) <https://www.ntnu.edu/ibt/about-us/what-is-biotechnology> accessed 20 January 2021
[5] Ray Hawk, 'What is red biotechnology?' (*Wisegeek*, 26 December 2020) < https://www.wisegeek.com/what-is-red-biotechnology.htm > accessed on 19 January 2021
[6] 'Red Biotechnology- The Saga of Medical Advancement' < http://www.biotech.in/red > accessed on 18 January 2021
[7] 'Biotechnology Industry in India' (*IBEF*, 31 December 2020) < https://www.ibef.org/industry/biotechnology-india.aspx > accessed on 15 January 2021
[8] 'Biotechnology Industry in India' (*IBEF*, 31 December 2020) < https://www.ibef.org/industry/biotechnology-india.aspx > accessed on 15 January 2021

Similarly, the use of organisms or human genomes in healthcare also poses serious and complicated ethical implications for the international community.

PART II: UTILITIES OF RED BIOTECHNOLOGY

1. REPRODUCTIVE MEDICINES

Infertility is considered as a social and economic disability as children play a significant role in providing social security to the family. Moreover, in the Indian scenario families often emphasize having biological children to ensure social continuity.[9] However, many couples are unable to conceive due to low sperm or oestrogen count, hostile nature of ovaries to the sperm and various other reasons. In India, approximately 17.9 million couples are infertile.[10] However, modern biotech has produced three popular methods for assisting in the process of reproduction, namely, (i). Artificial insemination (ii). *In vitro* fertilization often combined with cryopreservation and, (iii). Surrogacy.

In artificial insemination, a woman's ovum is fertilized by artificial insertion of semen of the husband of the woman or the donor. This process must be supplemented by using gametes via intrafallopian transfer to fertilize ova and sperm by putting them together in the fallopian tube.

Similarly, *In vitro* fertilization or IVF was developed by Robert Edwards, Patrick Steptoe and Jean Purdy. This is a procedure where sperm and ova are mixed in a test tube or a petri dish for inducing the process of fertilization. This fertilization results in the forming of pre-embryo which may be inserted in woman's womb or can be frozen to be used later by the process of crypto preservation.[11] In 1978, the first-ever child conceived through *In vitro* fertilization was born.

In surrogacy, the couple is not able to conceive due to the inhospitable nature of a person's womb. It can be dealt with by simply using either IVF or artificial insemination to put the pre-embryo inside another woman's womb who bears the capability to conceive.

[9] Sital Mohanty and Subhasis Sahoo, 'The ART of Manufacturing: Ethical Considerations in Quest of a Child' [2016] PL 380

[10] S. Ganguly and S. Unisa, 'Trends of Infertility and Childelessness in India: Finding from NFHS Data (*NCBI*, 2010) < https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4188020/ > accessed on 11 January 2021

[11] Sital Mohanty and Subhasis Sahoo, 'The ART of Manufacturing: Ethical Considerations in Quest of a Child' [2016] PL 380

Erectile Dysfunction is now treated by utilizing human penile tissues along with the nitric oxide and by an inhibitor of erectile GMP degradation.[12] Uterine leiomyomas have long been seen as an anathema to reproduction and the cause of gynecologic morbidity. Normal medicines have seen to have bothersome side effects on the health of the mother. In recent times, progesterone (P) found in pigs has proven to be a stimulator of estrogen myomas in the body of the mother which can subsume the effects of the uterine leiomyomas, reduce the pain and improve the quality of life.[13] Similarly, women who have lost their ovarian function due to chemotherapy or ovarian failure can cryopreserve ovarian tissues before chemotherapy and replace these tissues after the procedure of chemotherapy.[14]

2. ADVANCED BIOMEDICAL THERAPIES

The first instance of potential gene therapy was observed in 1972. Gene therapies are still considered to be in their experimental stage. The human genome resonates with a map which holds the navigation to the genetic codes of a human i.e. the relevant instructions for the development of the human being. However, these genomes are also responsible for causing many serious and potentially fatal diseases.[15] Intensive research in this area has allowed for the development of gene therapy which is the process of transferring healthy genes into tissues and cells which provides new instructions to cells or corrects any mutation caused by the patient's genome. This allows for healthy functioning of the cells and the tissues in the patient's body.[16]

The gene therapies are predominantly used to deal with haemophilia, immunodeficiencies and muscular dystrophies. However, gene therapies pose a danger of perturbed cell functions caused due to replacement of a defective cell.[17] A positive outcome of gene therapy is that hereditary diseases and defects can be cured today and more of them will be cured in the succeeding generations.

---

[12] Goldstein I, Lue TF, Padma-Nathan H, Rosen RC, Steers WD, Wicker PA, 'Oral sildenafil in the treatment of erectile dysfunction' [1998] PL 338

13 Haouzi D, Assou S, Mahmoud K, Tondeur S, Reme T, Hedon B, et al, 'Gene Expression Profile of Human Endometrial Receptivity: Comparison Between Natural and Stimulated Cycles For The Same Patients' [2009] PL 1436.

14 Oktay KH, Pacheco FS, 'Current Success and Efficiency of Autologous Ovarian Transplantation With Cryopreserved Tissue: A Meta-Analysis' [2016] PL 131

[15] Matthias Herdegen, 'From Test Tube Babies To Human Clones: Salient Issues in the International Law of Biomedicine' [2020] PL 80

[16] P.L. Chang (ed.), Somatic Gene Therapy (CRC Press, Boca Raton FL 2018); M. Giacca, Gene Therapy (Springer, Dordrecht 2010).

[17] M.C. Galli and M. Serabian, 'Regulatory Aspects of Gene Therapy and Cell Therapy Products: A Global Perspective [2015]

It also has various legal and ethical implications which will be discussed later in detail.

3. HUMAN CLONING

Cloning is the process of creating a physical and identical copy of a living being by growing tissues harvested from the original person.[18] Cloning remained a revolutionary idea with little success in actuation for most of the 20th century. The first successful animal cloning occurred in 1952 with the cloning of frogs by using cells from a tadpole embryo. Eventually, a breakthrough took place in 1953, when the structure of the DNA was determined. In 1996, the process of cloning was actuated for the first time in the history of mankind. In this experiment, a sheep named Dolly was cloned by harvesting mammary gland cells of a Finset Dorset ewe and fusing it with an unfertilized egg cell by using electrical impulses.[19] Before this, artificial cloning had been performed on frogs and other amphibians.[20] From thereon, the idea of human cloning i.e., cloning a human being has been taken with great interest by biologists due to its possible viability.

There are primarily two kinds of cloning: Reproductive and Therapeutic. Reproductive Cloning is the process of implantation of embryos into a uterus so that a baby carrying the identical genetic characteristic will be born. Therapeutic Cloning, on the other hand, is to create a cloned embryo by the procedure of Somatic Cell Nuclear Transfer (SCNT), that would be employed for therapeutic purposes such as deriving embryonic stem cells without pregnancy.

The potential of therapeutic cloning is a topic of intense discussion within the global community as a feasible way to produce cells, tissues or organs that are genetically compatible with patients to treat a range of diseases and physical injuries. However, at this juncture, it is better to refer to it as "research" cloning rather than "therapeutic" cloning.

The process of human cloning can be very well used to boost human abilities, to benefit mankind by recreating persons who had significant accomplishments in any

[18] Adv. Rakesh Vishan and Ms. Swati Vishan, 'Human Cloning: Perspective, Ethical Issues and Legal Implications' [2017] PL 70

[19] Judith L. Fridovich-Keil, 'Dolly Cloned Sheep' (*Britannica*, 3 December 2020) < https://www.britannica.com/topic/Dolly-cloned-sheep> accessed on 11 January 2021

[20] Francisco J. Ayala, 'Cloning Humans? Biological, Ethical and Social Considerations' (*PNSA*, 21 July 2015) < https://www.pnas.org/content/112/29/8879#sec-8> accessed on 14 January 2021

recognized virtue.[21] However, the human cloning presents a lot of policy and legal issues which needs to be made certain.

4. USING HUMAN EMBRYOS FOR RESEARCH

A human embryo is a product formed after the fertilization of the gametes.[22] After the process of fertilization, the embryo grows into a human being. By nature, human embryos are totipotent, which means that they can be developed into different forms of tissues by the process of 'differentiation'.[23] The use of human embryos in research and experimentation has the potential to have clinical value to deal with bodily injuries, diseases, enhancement of human abilities and enhancement of human endowments.[24] Some potential applications include (i) Development of specialized cell lines for drug toxicity and efficacy testing (ii) Research in the area of normal and abnormal differentiation and development (iii) Development of pluripotent stem cells and therapeutic use of specialized and differentiated cells. [25]

PART III: LEGAL FRAMEWORK GOVERNING RED BIOTECHNOLOGY

1. INTERNATIONAL LAW

Biotechnology has grown leaps and bounds over the past few decades. Owing to the revolution in this field, significant societal and policy issues have arisen. There are no two similar laws in the field of red biotechnology as all nation-states possess different capacities to develop, apply, as well as regulate the new biotech products and services. In terms of international relations, the United Nations has formulated certain declarations and conventions, such as the *Cartagena Protocol on Biosafety*, the *UN Convention on Biological Diversity, Agreement on Sanitary and Phyto-Sanitary Measures,* etc. There are several laws and conventions governing biotechnology in both international and municipal sphere. Since the area of biotechnology is vastly spread, there are certain umbrella legislation and there are sector-specific legislations.

[21] Anisha Bhandari, 'Human Cloning and Its legal aspects' (*Blog iPleaders*, 10 January 2021) < https://blog.ipleaders.in/human-cloning-legal-aspects/> accessed on 16 January 2021
[22] Committee on Pediatric Research and Committee on Bioethics, 'Human Embryo Research' [2001] PL 813
[23] *Ibid*
[24] *Ibid*
[25] *Ibid*

Three primary declarations govern the domain of bioethics: the 1997 *Universal Declaration on the Human Genome and Human Rights*, the 2003 *International Declaration on Human Genetic Data* and the 2005 *Universal Declaration on Bioethics and Human Rights*.

As far as human cloning is concerned, the *Nuremberg Code* and the *Declaration of Helsinki* are two significant guidelines for ethics in research involving human subjects. Since the cloning of Dolly, the Sheep in 1996, the question of whether human reproductive cloning should be permitted or banned has been the subject of prime importance in the international debate. In 2005, the United Nations adopted the *Declaration on Human Cloning* in its attempt to deal with the issue. However, problems arose eventually as the declaration is ambiguously worded and does not state which forms of cloning are prohibited. The Declaration prohibits *"all forms of human cloning since they are incompatible with human dignity and the protection of human life".* It received an indecisive response from the UN Members. Owing to this unsatisfactory outcome, UNESCO (the United Nations Educational, Scientific and Cultural Organization) set up a Working Group in 2008, to explore the possibility of formulating a legally binding convention to ban human reproductive cloning.

The Working Group discovered that the lack of lucidity in international law proved to be unhelpful for those states who were yet to formulate national rules or regulations on human cloning. It proved to be difficult for these States to define and construe the forms of cloning which would be incompatible with human dignity. All States possess different sets of ethos on their understanding of human dignity. Resultantly, these States would arrive at different conclusions concerning cloning practices they choose to ban.

The Working Group concluded that, although human reproductive cloning is a challenging subject, establishing a vigorous global governance framework in this area might be possible via an alternative deliberative format.

Several international and regional measures also prohibit human reproductive cloning such as the World Health Organization's resolutions of 1997 and 1998 focusing on the implications of cloning for human health, the European Council's 1998 *Additional Protocol to the Convention on Human Rights and Biomedicine, on the Prohibition of Cloning Human Beings* and the European Union's 2000 *Charter of Fundamental Human Rights*.

However, it is pertinent to note that there are no definitive international laws in the domain of red biotechnology, especially concerning human cloning. Moreover, in ***Evans vs. the United Kingdom***[26], the Court held that there was no international consensus concerning the regulation of IVF treatment or to the use of embryos created owing to such treatment. Different states have adopted different stands on various issues in the area of red biotechnology. Nonetheless, there seems to be a consensus among nations to prohibit human cloning.

2. INDIAN LAW

The Indian law about human cloning is on similar lines as that of international law. Biotechnology in its pristine form ushered into India in 1997 with the launch of rDNA technology-based product, the Hepatitis B vaccine. [27]

The existing regulatory framework in India comprises the Department of Biotechnology (DBT) formed under the aegis of Ministry of Science and Technology functions as the nodal agency for policy, promotion and international cooperation in the field of biotechnology. Along with DBT, the Genetic Engineering and Approval Committee (GEAC) is the leading regulatory authority in India. The Institutional Biosafety Committee (IBSC) is responsible for ensuring local implementation of guidelines. The Review Committee on Genetic Manipulations (RCGM) issues permits. These are certain authorities under the larger regulatory framework.

In 2010, the Central Drugs Standard Control Organisation constituted the Cellular Biotechnology Based Therapeutic Drug Evaluation Committee for reviewing cell therapy-based clinical trials in India.

In 2000, the Indian Council of Medical Research released '*Ethical Guidelines for Biomedical Research on Human Subjects.'* The document deals with concerns such as the possibility of commercial eugenics in the field of human genetics. It addresses issues such as human rights, issues of autonomy, human dignity and incompetency of human subjects to

[26] Evans v. United Kingdom, 43 E.H.R.R. 21
[27] 'Biotech Regulation in India: Problems and Premises' [2009] PL 306

provide informed consent. This policy document plays a major role in regulating clinical research in the domain of human genetics, the human genome and gene therapy.
Government of India's ethical policy on the human genome, genetic research and services prohibit reproductive cloning. However, doors to therapeutic cloning are considered on a case-by-case basis by the National Bioethics Committee.[28]

In the wake of the birth of the first baby born via *in vitro* fertilization in 1986; there was a huge spike in IVF clinics across India, functioning without requisite accreditation, regulatory mechanisms or the control of Indian Government. Resultantly, ICMR swung into action to formulate the *Draft National Guidelines for ART Clinics in India* in 2002. Subsequently, the Ministry of Health & Family Welfare scrutinized these guidelines and published the *National Guidelines of Government of India* in 2005.

Apart from this, the Government recently introduced the *Assisted Reproductive Technology (Regulation) Bill, 2020.* This Bill was introduced as a supplement to the *Surrogacy (Regulation) Bill, 2019.* This Bill envisages regulation of ART banks and clinics, laying down a proper procedure for safe and ethical practices of ARTs and protection of women and children from potential exploitation. However, it has been observed that the Bill is discriminatory, exclusive and infringes on the privacy of the individual. It is also in blatant disregard of Article 14 of the Indian Constitution. The Bill offers little for protection of the egg donor and the overall procedure of artificial insemination.[29]

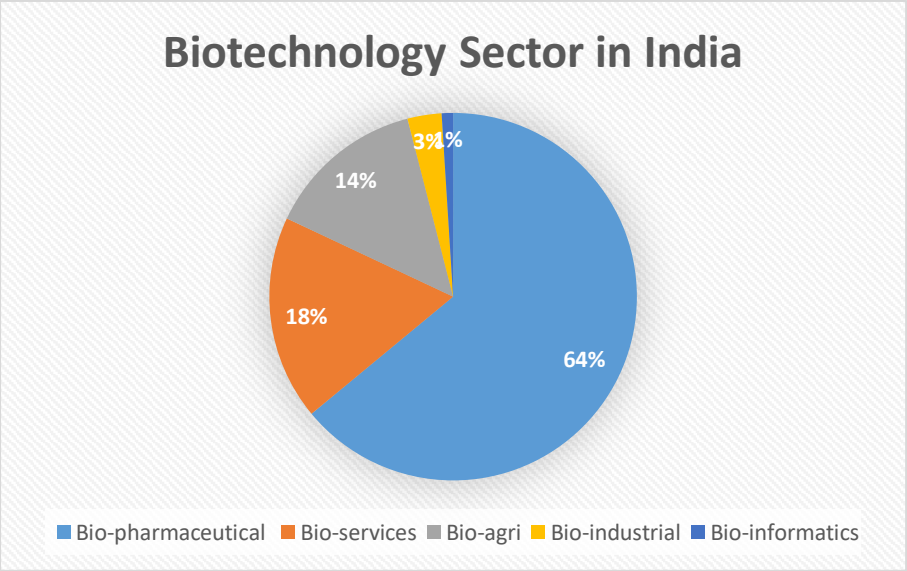
Other legislations include the *National Guidelines for Stem Cell Research, 2017* prepared by ICMR and DBT. These guidelines provide for stem cell research, the therapeutic use of stem cells, international collaboration, exchange of tissues, stem cells, etc. The *Guidelines for Generating Pre-Clinical and Clinical Data for r-DNA Vaccines, Diagnostics and Other Biologicals, 1999* deals with recombinant DNA technology and sets certain regulatory standards for r-DNA products. Additionally, the *Recombinant DNA Safety Guidelines, 1990* covers rDNA technology in vaccine development in its ambit. However, it excludes issues about Genetic Engineering of human embryos, their usage, etc. from its scope.

[28] Division of the Ethics of Science and Technology, 'National Legislation Concerning Human Reproductive and Therapeutic Cloning [2004]
[29] Prabha Kotiswarnan, 'Assisted Reproductive Technology Bill Needs a Thorough Review' *The Indian Express* (New Delhi, 9 October 2020)

It can be observed that the Indian regulatory system is divided instead of having an integrated, coordinated action in a holistic ecosystem.

PART IV: BIOTECHNOLOGY SECTOR IN INDIA

India is one of the emerging nations in the race of globalization and industrialization. The Government of India launched the 'Make in India' program in 2014 to attract investments from various multi-national entities across the world. Biotechnology sector forms a crucial part of the sectors identified by the Government. In the Indian market, the biotechnology sector is fundamentally divided into the following five segments[30] –



As a part of the Make in India campaign, incentives such as tax deduction for R&D expenditure, waiver of excise duty on patented products, setting up venture capital fund to assist MSMEs, etc. have been provided in the biotechnology sector. Owing to the establishment of biotech parks across the country, research and development have grown over the past few decades. The Government of India has taken several initiatives to ensure a conducive environment for the development of the sector. To catalogue the genetic variation in India, a project 'Genome India' was also launched.[31]

The Indian market is dynamic in its orientation and offers varied investment opportunities in the areas of drug discovery, clinical trials, medical devices manufacturing, etc.

[30] '6th World Congress on Biotechnology' [2015]
[31] Department of Biotechnology, 'Annual Report 2019-2020'

PART V: BIOETHICAL AND LEGAL IMPLICATIONS OF RED BIOTECHNOLOGY

Dolly's birth was the real breakthrough, as she was cloned from a fully differentiated adult mammary cell[32]. It generated controversies throughout the world because for the first time mammalian cloning and the potentials for human cloning became a reality[33]. Blastomere Separation and Nuclear Transfer are the most common methods of cloning. Blastomere Separation process involves taking an embryo soon after fertilization, generally at the two to the eight-cell stage[34], and separating the embryo into blastomeres. The nuclear transfer involves creating a new recipient cell by removing the DNA from an unfertilized egg cell, generating the most controversies and constituting the primary subjects of cloning legislations.[35]

The use of human embryos for research and therapeutic purposes is one of the most controversial issues of modern biotechnology. The use of embryos raises serious ethical and legal concerns about the 'instrumentalization' of human life, respect for human dignity, the protection of human rights and the privacy concerns.

1. HUMAN RIGHTS AND HUMAN DIGNITY

The fundamental rights enshrined in the Constitution, preserves and protect human dignity. The broad interpretation of Article 21, has interpreted the term 'life' to include all those aspects of life that are essential to make a person's life meaningful, complete, and worth living. The Supreme Court has emphasized human dignity as a fundamental right in several cases. In *Naz Foundation v. Government of NCT and Others*, the Court observed that "*the Constitutional protection of human dignity requires us to acknowledge the value and worth of all individuals as members of our society*".

Immanuel Kant's principle has always emphasized that an individual human life should never be thought of as only a means to an end, but an end itself, at all times[36].

[32] Roslin Institute Online, 'Nuclear Transfer: A Brief History'
[33] HGAC Papers, 'Cloning in Reproduction, Science and Medicine'
[34] Anne Lawton, 'The Frankenstein Controversy: The Constitutionality of a Federal Ban on Cloning' [1999] PL 277
[35] Khristan A. Heagle, 'Should There Be Another Elve? A Critical Analysis of the European Union Cloning Legislation' [1998] PL 144
[36] Carl J. Friedrich, 'The Philosophy of Kant: Immanuel Kant's Moral & Political Writings' [1999] PL 154

Creating cloned human life for the sole prerogative of its serving as a source of therapeutic material would not serve the dignity of life as advocated by Kant and provided by the Constitution of our country.

When cloning commodifies people and commodification demeans them, cloning demeans people by lessening their worth in society.[37] Dignity is reduced when society treats individuals as collections of body parts and dignity is similarly reduced when science is allowed to create clones of existing people. The view individuals have of themselves as potential clones, as well as the view society has of them if cloned, echoes the idea that people will feel commodified if they alienate their bodies.

The right to person's own identity is recognised in international law through various declarations and conventions. Article 19 of the *United Nation Declaration of Human Rights* and Article 10 of the *European Court of Human Rights* provides every individual with the right to freedom of opinion and expression. Macklem has explained that freedom of expression is not merely the freedom to communicate one's voice to others. It is the freedom to develop one's distinctive voice.[38] Thus, both these articles encourage the manifestation of personal identity. The Human Genetics Advisory Commission (HGAC) has defined cloning as producing a cell or organism with the same nuclear genome as another cell or organism'. Cloning in this aspect is said to breach a fundamental right to individuality. The uniqueness of identity and individuality are some of the most deep-felt and inherent signifiers of self. Just as a great artwork would lose their value in identical reproduction, so human beings can be said to lose their intrinsic inimitability in reproductions of themselves.[39]

The debates over biotechnology and its use in *In-Vitro* fertilization process centres upon the constitutional right to privacy.[40] Specifically, the question of whether the putative parents have the fundamental right to dispose of their embryos as they choose stems from the individual right to privacy. The judgment of *Puttuswamy v. Union of India* in India has ensured that the right to privacy is a fundamental right protected under Part III of the Constitution of India. The United State Supreme Court in *Eisenstadt v. Baird*[41] provided an

[37] NABER Report
[38] T Macklem, 'Independence of Mind' [2006] PL 11
[39] Gogarty, B, 'What exactly is an exact copy? And why it matters when trying to ban human reproductive cloning in Australia' [2003] PL 84
[40] Eisenstadt v. Baird, 405 U.S. 438 (1972)
[41] Eisenstadt v. Baird, 405 U.S. 438 (1972)

interesting explanation to this privacy right. It mentioned that "*If the right to privacy means anything, it is the right of the individual, married or single, to be free from unwanted governmental intrusion into matters so affecting a person as a decision whether to bear or beget a child*." Hence, the utilization of a new infertility technique falls under reproductive freedom.

Generally, this right to privacy has been implicated in the constitutional discussions relating to family, marriage, contraception, and abortion among other aspects.

2. ADDRESSING THE ETHICAL CONCERNS

The process of animal cloning experiments involves somatic cell nuclear transfer demonstrated that the efficiency of reconstituted eggs developing to generate a single live birth is currently very low. In cloning Dolly, 277 eggs were used, 29 started to divide, 9 induced pregnancy, but only 1 survived to term.[42] Another major concern that has been observed is the development of abnormalities, the large offspring syndrome has been a common problem occurring in several live-birth animals. In this syndrome, the offspring is born oversized with disproportionally large internal organs and often suffers from respiratory or circulatory problems.

In the artificial methods of reproduction, the conflict of greater good arises between the benefit of having a genetically identical child weighed and the ethical cost of potential developmental abnormalities. Besides, even though it is not so problematic as in therapeutic cloning, the status of surplus embryos in reproductive cloning is also controversial, as the procedure creates the possibility of more embryos being produced than are needed for implantation. After implantation of one to four of these cloned embryos, the surplus may be considered for cryostorage for future use or research and development activities. If the embryos are not used at all, then they would be destroyed. Even if all embryos are implanted into a woman, embryo reduction has to be performed for the sake of the healthy development of the others. Thus, the question arises what is the moral status of a human embryo?

The general observation is that an embryo is radically different from sperm or an egg, as it contains the DNA, the complete human genome.[43] That is, it has the potential to develop into a complete human being. Thus, the most widely agreed viewpoint holds that a human

[42] Farnsworth J, 'To clone or not to clone: the ethical question' [2002]
[43] Coors ME, 'Therapeutic cloning: from consequences to contradiction' [2002] PL 27

embryo is a potent symbol of human life that deserves profound respect.[44] The value attributed to a human embryo or foetus is key in determining whether it should be respected as an individual or not. While considering a human embryo as a potential human being and worthy of respect, its right to life should be recognized. As per the understanding of this perspective, it is ethically wrong to destroy human embryos[45].

PART VI: CONCLUSION AND SUGGESTIONS

Red Biotechnology is ubiquitous in modern healthcare. The trajectory of growth in this field only suggests that its presence would become bolder and more apparent with time. It has the potential to revolutionize healthcare and the way we interact with the environment around us. With the development of more sophisticated technology, researchers would be able to harvest different types of cells of animals and humans and manipulate them to treat even the deadliest diseases, increase the human abilities and senses, enhance the human endowments, make human clones, create genetically modified organs etc. The healthcare, in general, would be benefitted immensely from these developments.

However, the rapid development in the area of red biotechnology opens up unexplored paradigms for humanity. It opens the world to the idea of a dystopia where the balance of power among humans become lopsided due to physical and mental enhancements in capacities of humans. As discussed before, a lot of bioethical and legal issues and implications may arise which would then be needed to be dealt with swiftly. However, this is far from reality as the world leaders are befuddled and confused by this rather bittersweet development in biotechnology. This state of confusion also reflects in the legal framework for red biotechnology across the globe which seemingly is very vague and ambiguous in its ambit. There is no consensus even among the international community in the way to deal with the rapid advancement in biotech. Therefore, the law has not been able to keep up with the change in the human paradigms and it's the need of the hour to fill this gap.

Based on the serious moral and ethical concerns, the United Nations should adopt a binding resolution that prohibits all forms of reproductive cloning. The resolution should also allow for individual states to choose whether to permit therapeutic cloning based on their evaluation of whether the medical benefit outweighs the moral and ethical concerns. The

[44] Meyer JR, 'Human embryonic stem cells and respect for life' [2000] PL 166
[45] 'Ethical Issues Regarding Human Cloning: a nursing perspective'

resolution should include strict guidelines about regulations and procedures for those nations choosing to allow therapeutic cloning, to ensure the experiments stay within the bounds of what is ethically acceptable[46]

A flourishing Indian biotech sector reinforced by a comprehensive regulatory mechanism and a sympathetic political atmosphere would help India build a foundation to become a more prominent voice in global governance discussions concerning biotechnology. The adoption of a Bill like the Biotechnology Regulatory Authority of India which sets up a regulator for dealing with the dynamic issues in the areas would be a step in the right direction.[47]

[46] Channah Jarrel, 'No WORLDWIDE CONSENSUS: THE UNITED NATIONS DECLARATION ON HUMAN CLONING' [2003] PL 2015

[47] Vibha Ahuja, 'Regulation of Emerging Gene Technologies in India' (*NCBI,* 19 July 2018) < https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6069684/> accessed on 17 January 2021

BRAIN MAPPING (BMT) OR P300 TEST (FORENSIC SCIENCE)

Mehulkumar Rathod[1]

Abstract :

Brain Mapping is also called brain wave finger printing. Under this test the accused is first interrogated and asked certain questions to find out whether he is concealing some information or not. Thereafter sensors are attached to his head which is connected with the computer and he is shown certain images on computer or otherwise he is made to hear certain sounds. If he is familiar with those pictures and sounds the brain will react to them and the computer will record that. The images and sounds that are shown to him are called target stimuli. There are certain advantages/benefits of the Technique of Brain Mapping are :-

- Unambiguously identifies the perpetrators
- Differentiates the perpetrator from innocents and witnesses
- Upholds the right of innocents and prevent them from being the targets of lengthy and time consuming investigative procedures
- Possible to unearth criminal espionages
- Prevention of Future attacks by terrorist outfits.

Legal status: The technology of brain mapping developed has revolutionized the causes of crime investigation in the country and has obtained laurels and recognitions by the judiciary and Investigating agencies. Further, the Brain mapping technology has survived a series of legal challenges under article 20(3) and article 21 of Indian Constitution.

Brain Mapping (BMT) or P300 Test

It is called brain wave finger printing. Under this test the accused is first interrogated and asked certain questions to find out whether he is concealing some information or not. Thereafter sensors are attached to his head which is connected with the computer and he is shown certain images on computer or otherwise he is made to hear certain sounds. If he is familiar with those pictures and sounds the brain will react to them and the computer will record that. The images and sounds that are shown to him are called target stimuli. The subject is not asked any question during that test. The BMT result is matched with the information from the crime scene and if the

[1] Research Scholar, **Mehulrathod632@gmail.com**

matching is proper it is concluded that the accused has an information regarding crime. This goes against the accused.[2]

Things to be done prior to Brain Mapping :-

I. Identify and examine the proffered theory and hypothesis for their power to explain the data;
II. Examine the data that supports (and undermines) the expert's theory;
III. Use supportable assumptions to fill the inevitable gaps between data and theory;
IV. Examine the methodology
V. Engage in probabilistic assessment of the link between the data and the hypothesis.

Brain Mapping is defined as the study of the anatomy and functions of the brain and spinal cord through the use of imaging (including itra-operative, microscopic, endoscopic and multi-modality imaging), immune-histo-chemistry, molecular and optogenetics, stem cell and cellular biology.

Brain Mapping is a set of neuroscience techniques predicted on the mapping of (biological) quantities of properties onto spatial representations of the (human or non-human) brain resulting in maps. Brain Mapping is further defined as the study of the anatomy and function of the brain and spinal cord through the use of imaging (including intra-operative, microscopic, endoscopic and multi-modality imaging), immunohisto chemistry, molecular and optogenetics, stem cell and cellular biology, engineering (material, electrical and biomedical), neurophysiology and nanotechnology, according to the definition established in 2013 by Society for Brain Mapping and Therapeutics (SBMT).[3]

It measures the change in the electrical field potentials produced by the sum of the neuronal activity in the brain by means of electrodes placed on the surface of the skin covering the head and face. The changes directly related to specific perceptual or cognitive events are called event-related potentials. In simple words, it is based on the finding that the brain generates a unique brain-wave pattern when a person encounters a familiar stimulus. Commonly used

[2] Vij Niharika, *Law & Technology* (2015th edn, Universal Law Publishing Co Pvt Ltd 2015).
[3] SBMT means Society for Brain Mapping and Therapeutics

method in India is called as Brain Electrical Activation Profile test, also known as the 'P300 waves test'.

During the test, subjects are exposed to auditory or visual stimuli (pictures, videos and sounds) that are relevant to the facts being investigated alongside other irrelevant words and pictures. Such stimuli can be broadly classified as material 'probes' and neutral 'probes'. The underlying theory is that in the case of guilty suspects, the exposure to the material probes will lead to the emission of P300 wave components which will be duly recorded by the instruments. By examining the records of these wave components, the examiner can make inferences about the individual's familiarity with the information related to the crime. However, this measures only the memory or knowledge of the crime scene and nothing else. For instance, a by-stander who witnessed a murder could potentially by implicated as an accused if the test reveals that the said person was familiar with the information related to the same. Similarly, little is known about the impact of viewing portrayal of crime scene in the media such as television, movies and newspaper on brain mapping. Hence, this test cannot be used to prosecute an accused but can be used by an innocent as an 'alibi' by proving that he/she does not have any memory about the crime on this test.

There is a paucity of data on this technique, and applicability of this technique in the forensic field is remote at this point of time. There are several ongoing research studies using functional brain imaging studies in the field of brain mapping, however, results from these studies are also inconclusive and researchers have recommended that the functional brain images in brain mapping also should not be admitted as evidence in the court of law.

Nithari case, in which skeletons of 17 missing children were recovered from inside and near a house in Noida, house owner Mohinder Singh Pandher and his servant SurinderKoli were arrested and were made to undergo brain mapping and polygraph test in 2007.

History of Brain Mapping

In 1962 the origin of Brain Mapping Research was first started in Ohio, and conducted at the Columbus State Hospital. More than 500 subjects were scanned using the US patented

Brain Mapping

Hyper-frequency Electroencephalograph (Hyfreeg) brain scanner for the Brain Mapping Research. A detailed brain mapping report was published by the Battelle Memorial Institute "Is Nervous System Amplitude or Frequency Oriented?" JAMA reported: "One of the points on which most neurologist have agreed, is that the nervous system is amplitude oriented. Now a new theory indicates exactly the opposite – that the nervous system actually is frequency oriented." As a result of the brain mapping research, the psychiatric team members were able to cure: Epilepsy, Psychomotor Epilepsy, Hallucinations, and Schizophrenia by lowering the neuronal activity in the reticular Activating System located in the brain stem. They also observed the functions of Dreaming and the unique functions of the two brain hemispheres that was later confirmed by a girl born with only one hemisphere.

In the late 1980s in the United States, the Institute of Medicine of the National Academy of Science was commissioned to establish a panel to investigate the value of integrating neuro-scientific information across a variety of techniques. Following a series of meetings, the International Consortium for Brain Mapping (ICBM) evolved. The ultimate goal is to develop flexible computational brain atlases.[4]

Writing on the issue, MukeshYadav, the editor of the Journal of Indian Academy of Forensic Medicine, had pointed out that modern forensic techniques such as brain mapping, polygraph test, narco analysis and functional MRI are quite useful in revealing the truth from the accused.

"The brain mapping method scientifically detects the presence or absence of specific memories in the brain. Words, pictures, codes and sounds related to the crime are presented to the subject by a computer. The brain wave responses to these stimuli are measured using a headband equipped with EEG sensors. The data is then analysed to determine if the relevant information is present in the memory".

But this method too is not admissible

Advantages/Benefits of the Technique of Brain Mapping:-

[4] Jand D.S., *Forensic Science & Law* (New Era Law Publication 2019).

Brain Mapping

I. Unambiguously identifies the perpetrators.
II. Differentiates the perpetrator from innocents and witnesses.
III. Upholds the right of innocents and prevent them from being the targets of lengthy and time consuming investigative procedures.
IV. Possible to unearth criminal espionages.
V. Prevention of future attacks by terrorist outfits.

Drawbacks of the technique

DDT has faced a number of criticisms and it is still unclear to what degree lie detectors and brain mapping can be used to reveal concealed knowledge in applied real-world settings. The Supreme Court judgment on involuntary DDTs is that it has no place in the judicial process. On the contrary, it will disrupt proceedings cause delays, and lead to numerous complication which will result in no greater degree of certainty in the process than that which already exists.

The vulnerability of the techniques to countermeasures also needs to be explored. It is also important to know the sensitivity and specificity of these tests. There should be standard operating guidelines for conducting DDT.

For use as a forensic tool, a procedure needed to have established error rates. But brain mapping as done in the Forensic Science Laboratories (FSL) in Bangalore and a variation called Brain Electrical Oscillation Signature (BEOS) profiling in Gandhinagar, Gujarat, had not worked on this factor. The recent Supreme Court judgement on DDT is admirable from the scientific, human rights, ethical, legal and constitutional perspectives.

Brain Mapping techniques are constantly evolving, and rely on the development and refinement of image acquisition, representation, analysis, visualization and interpretation techniques. Functional and structural neuro-imaging are at the core of the mapping aspects of brain mapping. All neuro-imaging can be considered part of brain mapping. Brain Mapping can be conceived as a higher form of Neuro-imaging, producing brain images supplemented by the result of additional (imaging or non-imaging) data processing or analysis, such as maps projecting (measures of) behaviour onto brain regions. One such map, called a connectogram,

depicts cortical regions around a circle, organized by lobes. Concentric circles within the ring represent various common neurological measurements, such as cortical thickness or curvature. In the center of the circles, lines representing white matter fibers illustrate the connections between cortical regions, weighted by fractional anisotrophy and strength of connection.

On May 5, 2010 the Supreme Court in India (Smt. Selvi v. State of Karnataka) declared brain mapping, lie detector tests and narco-analysis to be unconstitutional, violating Article 20(3) of Fundamental Rights. These techniques cannot be conducted forcefully on any individual and requires consent for the same. When they are conducted with consent, the material so obtained is regarded as evidence during trial of cases according to section 27 of the Evidence Act.

Brain Electrical Activation Profile (BEAP) Test

Another technique in question is the "Brain Electrical Activation Profile test" also known as the 'P300 Waves test'. It is a process of detecting whether an individual is familiar with certain information by way of measuring activity in the brain that is triggered by exposure to selected stimuli. This test consists of examining and measuring 'event-related potentials' (ERP) i.e. electrical wave forms emitted by the brain after it has absorbed an external event. An ERP measurement is the recognition of specific patterns of electrical brain activity in a subject that are indicative of certain cognitive mental activities that occur when a person is exposed to a stimulus in the form of an image or a concept expressed in words.

The measurement of the cognitive brain activity allows the examiner to ascertain whether the subject recognised stimuli to which he/she was exposed.

By the late 19th century it had been established that the brain functioned by emitting electrical impulses and the technology to measure them was developed in the form of the electroencephalograph (EEG) which is now commonly used in the medical field. Brain wave patterns observed through an EEG scan are fairly crude and may reflect a variety of unrelated brain activity functions. It was only with the development of computers that it became possible to sort out specific wave components on an EEG and identify the correlation between the waves and specific stimuli. The P300 wave is one such component that was discovered by Dr. Samuel Sutton in 1965. It is a specific event-related brain potential (ERP) which is triggered when

information relating to a specific event is recognised by the brain as being significant or surprising.

The P300 waves test is conducted by attaching electrodes to the scalp of the subject, which measure the emission of the said wave components. The test needs to be conducted in an insulted and air-conditioned room in order to prevent distortions arising out of weather conditions.

The P300 wave test was the precursor to other neuro scientific techniques such as 'Brain Fingerprinting' developed by Dr. Lawrence Farwell. The latter technique has been promoted in the context of criminal justice and has already been the subject of litigation. There is an important difference between the 'P300 waves test' that has been used by Forensic Science Laboratories in India and the "Brain Fingerprinting' technique. Dr. Lawrence farwell has argued that the P300 wave component is not an isolated sensory brain effect but it is part of a longer response that continues to take place after the initial P300 stimulus has occurred. This extended response bears a correlation with the cognitive processing that takes place slightly beyond the P300 wave and continues in the range of 300-800 milliseconds after the exposure to the stimulus. This extended brain wave component has been named as the MERMER (Memory – Encoding-Related Multifaceted-Electroncephalographic Response) effect.

CBI recently decided to send a team to Bhopal to put several of the suspects in the Vyapam admission scam through a polygraph (lie detection) test by the end of September, in order to give them chance to prove their "Innocence". This has brought into the spotlight the issue of scientific evidence and its admissibility in the court of law.

The important part is that the CBI has not forced any of the suspects to take these tests. The law pertaining to the use of polygraph is very clear – the authorities cannot subject any accused or suspect to undergo narco analysis, brain mapping or polygraph test forcibly.

Brain Mapping

In May 2010, the Supreme Court held that forcing suspects and witnesses to take these tests without their consent was unconstitutional and amounted to violation of their right to privacy.

A three-judge bench had held that "the compulsory administration of the impugned techniques violates the right against self-incrimation.

Legal Status

The technology of brain mapping developed has revolutionized the causes of crime investigation in the country and has obtained laurels and recognitions by the judiciary and Investigating agencies. Further, the Brian Mapping technology has survived a series of legal challenges under article 20(3) and article 21 of Indian Constitution.

Power of High Court in Conducting Brain Mapping Test.

The court adjourned the matter at the instance of the learned senior advocate appearing on behalf of the petitioner so as to enable the petitioner to move an appropriate application before the Hon'ble Supreme Court for transfer of the present proceedings and on the last occasion it was agreed by the learned counsel appearing on behalf of the petitioner that if no orders are obtained he will proceed further with the matter and make submissions on merits. The petitioner is not desirous of submitting an appropriate application for transfer before the Hon'ble Supreme Court and that is how this Court has taken up the matter and considered the same on merits. It is also required to be noted that conducting/performing of the aforesaid two tests are timely requirement, more particularly during the course of the investigation and if after the period of 6 months or so and/or after a long time, the said test are permitted to be performed, the purpose for which the said tests are required would be frustrated. If the said tests are not permitted to be performed at an appropriate time and stage, the same would defeat the purpose for which the said test is required to be performed i.e. to find out the truth to reach the real culprit and to further investigate the case. There are so many proceedings pending in the State involving serious offences like Sorabuddin encounter case and the murder of his wife Kausharbibi and others. Where the questions with regard to conducting/performing of the Brain Mapping Test is involved and in some cases the Investigation Agency have found themselves in dark and clueless, there is necessity of conducting the Brain Mapping Tests and the proceedings are

pending at different stages before the different courts i.e. either at the stage of learned Magistrate and/ or Revisional Court and or before this court and therefore, this court has considered the case on merits.

Santokben Sharman bhaiJadeja v. State of Gujarat[5]

The right to direct the accused to undergo scientific tests has been finally determined by the Court below and thereby the criminal proceedings taken to demystify the grey area of investigation has culminated. Therefore, the Court finds that the present order impugned which substantially determines the rights of the parties is a final order challengeable under Section 397 of the code of Criminal Procedure by way of revision – Dinesh Dalmia v. State.[6]

Supreme Court Judgement on Plygraph, Narco Analysis & Brain Mapping – A Bane or Boon?

The deception detection tests (DDT) such as pplygraph, narco-analysis and brain-mapping have important clinical, scientific, ethical and legal implications. The DDT are useful to know the concealed information related to crime. This information, which is known only to self, is sometimes crucial for criminal investigation. The DDTs have been used widely by the investigating agencies. However, investigating agencies know that the extracted information cannot be used as evidence during the trial stage. They have contested that it is safer than 'third degree methods' used by some investigators. Here, the claim is that, by using these so called. "scientific procedures" in fact-finding, it will directly help the investigating agencies to gather evidences, and thereby increase the rate of prosecution of the guilty and the rate of acquittal of the innocent. Recently, these methods are being promoted as more accurate and best to none, without convincing evidence. In a landmark judgement, the apex court of India has clearly stated that DDTs cannot be administered without consent.

(A) Recent Supreme Court Judgement on DDTS

The Supreme Court judgement on May 5, 2010 relating to the involuntary administration of DDT for the purpose of improving investigation efforts in criminal cases was questioned on the account of violation of fundamental rights such as:

[5] *Santokben Sharman bhai jadeja v state of gujarat* (2009) 68.
[6] *Dinesh Dalmia v state of Madras* (2006) 2401.

Brain Mapping

(I) 'Right against self-incrimation' enumerated in Article 20(3) of the Constitution, which states that no person accused of an offence shall be compelled to be a witness against himself/herself, and

(II) Article 21 (Right to life and personal liberty) has been judicialllyexpanded to include a 'right against cruel, inhuman or degrading treatment'.

DDT also raises serious concerns related to the professional ethics of medical personnel involved in the administration of these techniques and violation of human rights of an individual. Concern regarding human rights violation in conducting DDTs were raised long back and the National Human Rights Commission had published Guidelines in 2000 for the Administration of Polygraph tests. However, only few of the investigating agencies have been seen to follow these guidelines.

(B) Use of Narco-Analysis, Brian-Mapping Unconstitutional declared by Supreme Court

Use of Narco-analysis amounts to unwarranted intrusion into personal liberty, a three-judge Bench of the Supreme Court said on Wednesday. In a major blow to investigating agencies, the Supreme Court on Wednesday held unconstitutional and violation of the 'right to privacy' the use of narco-analysis, brain mapping and polygraph tests on accused, suspects and witnesses without their consent.

A three-judge Bench of Chief Justice K.G. Balkirshnan and Justice R.V. Raveendran and J.M.Panchal, in a 251-page judgement, said: "We hold that no individual should be forcibly subjected to any of the techniques in question, whether in the context of investigation in criminal cases or otherwise. Doing so would amount to an unwarranted intrusion into personal liberty."

The Judges said: "The compulsory administration of the impugned techniques violates the right against self-incrimination. The test results cannot be admitted in evidence if they have been obtained through the use of compulsion. No person accused of any offence shall be compelled to be a witness against himself protect an individual's

choice between speaking and remaining silent, irrespective of whether the subsequent testimony proves to be inculpatory or execulpatory".

The Bench said:Article 20(3) aims to prevent the forcible conveyance of personal knowledge that is relevant to the fact in issue. The results obtained from each of the impugned tests bear a testimonial character and they cannot be categorised as material evidence."These concerns have been recognised by Indian Judiciary as well as foreign judicial precedents in **State of Bombay v. KathiKaluOghad.**[7]

Secondly, the ambit of the words 'accused of any offence' in Article 20(3) must be examined – i.e. whether the protection is available only to person who are formally accused in criminal cases, or does it extend to include suspects and witnesses as well as those who apprehend incrimination in cases other than the one being investigated?

Thirdly, the evidentiary value of independent materials that are subsequently discovered with the help of the test results is to be evalued. In light of the 'theory of confirmation by subsequent facts' incorporated in section 27 of the Indian Evidence Act, 1872 we need to examine the compatibility between this section and Article 20(3). Of special concern are situations when persons could be compelled to reveal information which leads to the discovery of independent materials. To answer this question, we must clarify what constitutes 'incrimination' for the purpose of invoking Article 20(3).

(C) Applicability of Article 20(3) to the stage of investigations

The question of whether Article 20(3) should be narrowly construed as a trial right or a broad protection that extends to the stage of investigation has been conclusively answered by our courts. In **M.P.Sharma v. Satish Chandra**[8]**,** it was held by Jagannadhadas, J. "Broadly stated, the guarantee in Article 20(3) is against 'testimonial compulsion'.

[7] *The State Of Bombay vs Kathi Kalu Oghad And Others* (1961) 1808 Bombay High Court.
[8] *M P Sharma And Others vs Satish Chandra* (1954) 300.

These observations were cited with approval by B.P.Sinha, C.J. in **State of Bombay v. KathiKaluOghad& Others.** In the minority opinion, Das Gupta, J. affirmed the same position, Id. At p.40: "…If the protection was intended to be confined to being a witness in court then really it would have been an idle protection. It would be completely defeated by compelling a person to give all the evidence outside court and then, having what he was so compelled to do proved in court through other witnesses. An interpretation which so completely defeats the constitutional guarantee cannot, of course, be correct. The condition that the protection afforded by Article 20(3) is limited to the stage of trial must therefore be rejected

ETHICAL ISSUES IN CYBERSPACE: A JURISPRUDENTIAL APPROACH

Ms. Kavita Bhatia[1] & Dr. Archana Gadekar[2]

Abstract:

Ethics is inseparable part of any civilised society. Ethics places norms that how to live best as a human being. The ethical values are more important when no one is supervising one's behaviour but still, he or she is expected to follow some basic ethics while performing social, economic and political duties. The technological advancement plays a greater role in transforming the social engagement of people. The way in which the technology has occupied the space in day-to-day life, the security norms to keep people's personal life, personal is a great challenge. The law related to cyberspace provides the code of conduct that, how to use the technology. But the technology is growing with a great speed and to regulate the same is also a challenge. This paper would examine the ethical issues relating to cyberspace. And the paper would also examine that how theories of jurisprudence would help an individual to understand the ethical values while using the technology.

Introduction

Cyberspace is a non-physical space enabled by the technology upon which the Internet operates. It occupies major space in our social and economic endeavours. Hence, Cyber ethics has to be determined so as to consider the fair use of technology. Cyber ethics, aims to protect Internet users through legal safe-guards in cyberspace. The legal safeguard is only possible be through basic ethical values observed by Internet users. It is bitter to accept that the way in which the internet users are increased as mushroom growth the Cyber-crimes have also become increasingly common in recent years. The cyber jurisprudence which comprises the existing bodies of law, including the law of war, international treaties, and domestic criminal law through which cyber-attacks would get regulated. This Article concludes that a new, comprehensive ethical based legal framework at both the domestic and international levels is needed to address cyber-crimes more effectively. According to Salmond, a perfect right is one which corresponds

[1] Assistant Professor, Faculty of Law, The Maharaja Sayajirao University of Baroda, Vadodara
[2] Associate Professor, Faculty of Law, The Maharaja Sayajirao University of Baroda, Vadodara

to a perfect duty[3]. An antecedent right is one which exist irrespective of any wrong have been committed. It is an exceptional advantage granted to the person who is clothed with this right. For instance, purchaser of internet services has an antecedent right over the services so purchased[4]. In recent time right to access internet is one of the essential rights which is to be established as a fundamental right as human life is so much dependable on technology. The access of safe internet is required to be considered as fundamental right. Unfortunately, this right is based on economic resources available to a person. Some people have access of internet but does not able to get it safe from cyber-attack as it requires added economic resources which is more costly than the access of internet services. This paper would discuss the right to use internet, which is based on economic condition of person, should be based on ethical behaviour of a person. Some ethical duties which have to be complied with while using internet and non-complying with these basic ethics would lead debarred him/her from the services of internet in addition to other criminal punishment set under various provision of legislations.

Ethical Norms: Cyberspace

Ethics denotes code of conduct. It cannot be undermined even while exercising legal right. The performance of legal right must be followed by ethics. Ethics, also called moral philosophy, the discipline concerned with what is morally good and bad and morally right and wrong. Its subject consists of the fundamental issues of practical decision making, and its major concerns include the nature of ultimate value and the standards by which human actions can be judged right or wrong. The terms ethics and morality are closely related[5].

Virtue approaches to ethics are found in the ancient Greek and Roman traditions, in Confucian, Buddhist and Christian moral philosophies, and in modern secular thinkers like Hume and Nietzsche. Virtue ethics focuses not on rules for good or bad actions, but on the qualities of morally excellent persons (e.g., virtues). Such theories are said to be character based, insofar as they tell us what a person of virtuous character is like, and how that moral character develops. Such theories focus on the habits of action of virtuous persons, such as the habit of moderation (finding the ‘golden mean’ between extremes), as well as the virtue of prudence or

[1] Dr. N.V. Paranjape, Study in Jurisprudence and Legal Theory, (Eighth edn. Central Law Agency) 401.
[2] Paranjape, Study in Jurisprudence and Legal Theory, (n.1) 430.
[3] Peter Singer, ‘Ethics’,<www.britannica.com/topic/ethics-philosophy>accessed 5th January 2021.

practical wisdom (the ability to see what is morally required even in new or unusual situations to which conventional moral rules do not apply)[6].

Ethics can be viewed from two angles, normative and prescriptive. First, ethics refers to well-based standards of right and wrong that prescribe what humans ought to do, usually in terms of rights, obligations, benefits to society, fairness, and specific virtues. Ethical standards also include those that enjoin virtues of honesty, compassion, and loyalty. Secondly, ethics refers to the study and development of personal ethical standards, as well as community ethics, in terms of behaviour, feelings, laws, and social habits and norms which can deviate from more universal ethical standards. So, it is necessary to constantly examine one's standards to ensure that they are reasonable and well founded. Ethics also means, then, the continuous effort of studying of our own moral beliefs and conduct, and striving to ensure that we, and our community and the institutions we help to shape, live up to standards that are reasonable and solidly-based for the progress of human beings[7].

Proper behaviour of ICT users refers to the specific actions required by the norm of the community. Some norms are regulative in character, creating duties or obligations that prescribe, prohibit, or permit some activity (or inactivity). Others are generative or constitutive: they create new rights or even new actors. Regulatory cyber norms are already extensive in cyberspace, whether as prohibitions on behaviour such as cybercrime or the use of force in cyberspace; duties such as requiring assistance to victims of severe cyberthreats; or permissions such as the use of TCP/IP[8].

"Cyber ethics" refers to the code of responsible behaviour on the Internet. Just as we are taught to act responsibly in everyday life with lessons such as "Don't take what doesn't belong to you" and "Do not harm others," we must act responsibly in the cyber world as well. The basic rule is *" Do not do something in cyberspace that you would consider wrong or illegal in everyday life*[9]*."*

[4] Shannon Vallor, William J. Rewak, 'An Introduction to Cybersecurity Ethics', <https://www.scu.edu/media/ethics-center/technology-ethics/IntroToCybersecurityEthics.pdf> accessed 5th January 2021.
[5] Avani Yadav, 'Cyber law and Ethics' (2017)<http://kanoon.nearlaw.com/2017/10/26/cyber-law-and-ethics> accessed 7th January 2021.
[6] Martha Finnemore and Duncan B. Holli, Constructing Norms for Global Cybersecurity, The American Journal of International Law, Vol. 110, No. 3 (July 2016), pp. 425-479.
<https://www.jstor.org/stable/10.5305/amerjintelaw.110.3.0425> accessed 12th January 21.
[7] Centre for Internet Security, <https://www.cisecurity.org/daily-tip/know-the-rules-of-cyber-ethics> accessed 7th January 2021.

Theories of Jurisprudence

Deontological ethics are rule or principle-based systems of ethics, in which one or more rules/principles are claimed to tell us what our moral obligations are in life. The 18th century philosopher Immanuel Kant, who identified a single moral rule called the categorical imperative. He contemplates that never to treat a human being as a 'mere means to an end,' that is, as an object to be manipulated for our own purposes. For example, I might want to tell a lie to get myself out of trouble in a particular case. But I certainly would not want everyone in the world to lie every time they felt like it would help them avoid trouble. And if someone lies to me to get me to do something that benefits them, I am rightly upset about being treated as a mere object to be manipulated for gain. So, "I cannot logically give myself permission to lie, since there is nothing about me that exempts me from my own general moral standards for human behaviour. For if I am willing to give myself permission to act in this way for this reason, how could I logically justify withholding the same permission from others?" According to this principle, human lives are the ultimate sources of all moral value. It implies universal moral obligation to treat other human lives in ways that acknowledge and respect their unconditional value, and to not treat them merely as tools to manipulate for lesser purposes. And since, "I myself am human, I cannot morally allow even my own existence to be used as a mere tool for some lesser purpose (for example, to knowingly sell out my personal integrity for money, fame or approval)"[10].

Austin assumes that law (in the second sense) is a body of rules[11] and insist vigorously on this separation of law and morals. Maine was often much influenced by Austin. He is zealous, in the maturity of law, to point out that a legal right is not necessarily right in the ethical sense-that it is not necessarily accordant to our feelings of what ought to be. He is zealous to show that a man may have a legal right which is morally wrong, and to refute the proposition that a legal right is not a right unless it is right. Kant made a clear distinction. He begins with a proposition that man, in endeavouring to bring his animal self and his rational self into harmony, is presented to himself in two aspects, an inner and an outer, so that his acts have a twofold aspect. He asserts

[8] Martha Finnemore and Duncan B. Holli, Constructing Norms for Global Cybersecurity, The American Journal of International Law, Vol. 110, No. 3 (July 2016), pp. 425-479. <https://www.cambridge.org/core/journals/american-journal-of-international-law accessed 12th January 2021.

[11] Austin's first assumption, taken from Bentham.

that “The law has to do with his acts in the former aspect, morals have to do with them in the latter aspect. The task of the law is to keep conscious free-willing beings from interference with each other. It is so to order their conduct that each shall exercise his freedom in a way consistent with the freedom of all others, since all others are to be regarded equally as ends in themselves. But law has to do with outward acts. Hence it reaches no further than the possibility of outward compulsion. There is a right in a legal sense only to the extent that others may be compelled to respect it[12].

In philosophical jurisprudence, with the rise of the social philosophical school, theories of legal precepts as having for their end the realization of moral precepts, revive to some extent the old subordination of jurisprudence to ethics. This begins with Jellinek as far back as 1878. Law, he said, was a minimum ethics. That is, 'the field of law was that part of the requirements of morals, observance of which is indispensable in the given stage of social development. By "law" here (Recht) he meant law as we try to make it or in its idea. The actual body of legal precepts may fall short of or in places or at times may go beyond this ethical minimum. So regarded, law is only a part of morals. That is, the field of law is only a part of the field of ethical custom, namely, the part which has to do with the indispensable conditions of the social order[13].

According to Jhering, the social utilitarian, “the immediate task of the law is to secure interests. Therefore, we must choose what interests we will recognize, fix the limits within which we will recognize them, and must weigh or evaluate conflicting or overlapping interests in order to secure as much as we may with the least sacrifice. In making this choice and in weighing or evaluating interests, whether in legislation or in judicial decision or in juristic writing, whether we do it by law making or in the application of law, it is said that we must turn to ethics for principles[14].

Stammler, the leader of the Neo-Kantians, “we seek justice through law and he comes finally to the proposition that "just law has need of ethical doctrine for its complete realization." As Kohler, the leader of the Neo-Hegelians put it, government, law, and morality are forces

[12] Roscoe Pound, ‘Law and Morals - Jurisprudence and Ethics’, North Carolina Law Review, Volume 23, Number - 3, Article- 1. < https://scholarship.law.unc.edu/nclr/vol23/iss3/1/> 26 January 2021.
[13] ibid.
[14] ibid.

working toward the attainment of an ideal of civilization. So, jurisprudence, he says, "must appreciate these ideal ends toward which society strives." To him jurisprudence and ethics are both subordinated to a universal history of civilization from which we determine the course of -development of civilization and to a philosophy of right and of economics from which we determine the jural postulates-the presuppositions as to right conduct -of the civilization of the time and place[15]. Morals have to do with thought and feeling, while the law has to do only with acts; that in ethics we aim at perfecting the individual character of men, while law seeks only to regulate the relations of individuals with each other and with the state. Vinogradoff, much more historian than jurist, as to law and "custom," i.e., ethical custom or morality. He proceeds, "In the term *right* itself the moral and the juridical connotations are indissolubly connected; both personal claim [subjective right] and social order [objective right] have their root in moral sense-in the ethics of social intercourse[16].

In recent time cyber domain has challenged the traditional, political, social and economic structures of the international society. It has radically increased the speed, volume and range of communication. The Concept of 'Cyber Governance' and 'Cyber Ethics' should be elaborated by keeping in mind the theories of jurisprudence based on ethics.

Cyberspace Jurisprudence

Cyber jurisprudence may be described as the specifics of law applicable to cyberspace, where the cyberspace is to be understood as the transnational platform for simultaneous interactions among Internet users. Cyberspace is a non-physical space enabled by the technology upon which the Internet operates. Cyber jurisprudence therefore needs to recognize the transboundary, mass, and simultaneous nature of all human interactions enacted in cyberspace. It aims to protect through legal safe-guards the values shared in cyberspace. This can be achieved after the basic ethical values shared by Internet users and significant for electronic communications are identified. The focus of jurisprudence is therefore to identify common values in need of specific legal protection in cyberspace, to identify cyberspace-specific threats

[15] Roscoe Pound, 'Law and Morals - Jurisprudence and Ethics', North Carolina Law Review, Volume 23, Number - 3, Article- 1. < https://scholarship.law.unc.edu/nclr/vol23/iss3/1/> 26 January 2021.

[16] Ibid.

to those values and analyse them and also individually asses those threats according to various normative systems and to verify the need for introducing additional, specific legal safeguards - cyberspace specific laws not only that to identify the ways of successfully safe-guarding those interests by recognizing the characteristics of cyberspace and its multi stakeholder environment[17].

The Information Technology Act, 2000 provides the regulatory mechanisms to report cyber-crime in India. It is detailed law that deals with technology with respect to e-governance, e-commerce, and e-banking. The Act also lays down penalties and punishments for cyber-crime in India.

As cyber technology transitions from the ICTs of the early twenty-first century to the digital world, the UN Secretary General's initiative to convene a multi-stakeholder High-level Panel for identifying areas for Digital Cooperation provides a launching pad for the UNGA (UN General Assembly) to create an appropriate international framework for cyberspace. In December 2019, the UNGA adopted a resolution moved by Russia on countering "the use of information and communication technologies for criminal purposes." According to the Russian delegation, the next step would be for the UNGA to hold an "organizational session in New York in 2020," with negotiations on the text of "a comprehensive international convention on countering cybercrime" starting in 2021. The resolution sets the stage for the first inter-governmental negotiation in the UNGA on creating a legal framework to counter cybercrime. With its narrow focus on cybercrime, the proposed legal framework would be potentially falling short of the "holistic" approach towards securing cyberspace that is emerging as a template in international multi-stakeholder discussions[18].

Suggestions

To overcome from the issues related to cyber security, professional training can be a powerful way to ensure values embedded in the norm which are inculcated into key actors in organizations and into the policies that they implement. An example from cybersecurity involves the U.S. Telecommunications Training Institute, which offers training to regulators,

15 Joanna Kulesza, Cyber jurisprudence, Jahrbuch für Recht und Ethik, Annual Review of Law and Ethics, Vol. 23,Themenschwerpunkt: Recht und Ethik im Internet Law and Ethics on the Internet (2015), 361-376.< https://www.jstor.org/stable/45176637> accessed 12th January 2021.

18 Asoke Mukerji, The Need for an International Convention on Cyberspace, Horizons: Journal of International Relations and Sustainable Development, No. 16, Pandemics & Geopolitics: The Quickening (SPRING 2020), 198-209

professionals, and entrepreneurs from the developing world. Another mechanism is Socialization is to punish ICT violators and the norm violators and they should be labelled as "rogues" who are not to be trusted, thereby threatening their status and their reputations. "Naming and shaming" of norm violators is a well-known tool of activists seeking to promote norms—one available even to weak actors seeking to change behaviour of much more powerful parties like states or big multinational firms. Publicizing names of norm violators can inflict reputational costs and compromise the credibility of violators in ways that are in some sense coercive, but any behavioural changes are actually achieved through speech and social relations rather than material incentives.

Conclusion

ICTs are now woven into every facet of human activity, from operating nuclear arsenals to raising cows. But for all their benefits, ICTs present an array of new opportunities for causing harm. ICT controls personal data and financial assets and intellectual property may be stolen through cyber-attack. Cyber insecurity has become the new normal, making cybersecurity a global priority not just for ICT companies but for nation-states, industry, and users generally. As states and stakeholders wrestle over when and how to preserve cybersecurity, they are increasingly turning to norms as the policy tool of choice to ensure cybersecurity for ICTs and cyberspace more generally[19].

Social media is fast becoming the preferred mode for education, employment, commerce and personal expression. Indeed, non-access and disconnection from the internet has been described as tantamount to 'non-existence'. The internet is 'inherently democratic' because it provides the public with access to information and enables individuals to actively participate in the process of communication[20]. The ICT is a powerful tool for spreading misinformation, propaganda, and hateful messages. The catastrophe is it is difficult to draw the line between robust debate which advances knowledge-creation and speech that harms civic deliberations.

[17] Martha Finnemore and Duncan B. Holli, Constructing Norms for Global Cyber security, The American Journal of International Law, Vol. 110, No. 3 (July 2016), 425-479. <https://www.cambridge.org/core/journals/american-journal-of-international-law accessed 12th January 2021.

[18] The United Nations (UN) Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Mr Frank La Rue has been mandated to provide his views on the advantages and challenges of new information and communication technologies, including the internet and mobile technologies.

This situation is critical, and these dangers and risks has to be adequately addressed by regulation.

Further, the rapid evolution of technologies increases issues related to cyber security in cyber space. cyber-space as "the fifth domain of warfare" after ground, sea, air and space, the need to have practical rules regulating all aspects of cyber-warfare activities –especially from the point of view of international law – has become a priority for all international actors. The complexity of the subject makes this task particularly challenging. A cyber-attack can be defined as an "armed attack". The challenges that governments, the Armed Forces and National Security Institutions are, and will be, facing increasingly in the field of cyber-security and cyber intelligence are certainly as complex as they are fascinating. Cyber-weapons require an adaptive response approach, which includes both the technical-technological research sector and the strategic, operational, and tactical sectors[21]

[19] Stefano Mele, Legal Considerations on Cyber-Weapons and Their Definition, , Journal of Law & Cyber Warfare, Vol. 3, No. 1 (Spring 2014), 52-69. < https://www.jstor.org/stable/26432559> accessed 12th January 2021

NAVRACHANA UNIVERSITY

a UGC recognized University

Designed and Arranged by:
PRAYRANA SINGH
5th Year Student,
Navrachana University

PUBLISHED BY

Navrachana University in association with Gujarat National Law University