JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

ADDRESSING LEGAL GAPS: SAFEGUARDING HUMAN RIGHTS IN THE AGE OF EMERGING TECHNOLOGIES

Mr Pratham Kumar [1] & Dr Shibu Puthalath[2]

Abstract:

This research offers a distinctive perspective on the development of technological applications and their impact on human rights concerns. New-age technologies such as AI, blockchain, and biotech have outpaced the development of legal frameworks, resulting in a "legal vacuum" on these technologies. In the absence of any comprehensive regulation, human rights are severely at risk. This paper aims to consider the consequences of such a legal vacuum, with particular emphasis on privacy, freedom of expression, and security of individuals. It underlines that, in the context of developing technological changes, there is an urgent need to develop specific legal standards to protect such human rights. The paper aims to determine the scope of the legal vacuum in those technologies, analyze the effects of the technologies on human rights, and analyze the role of international organizations in the regulatory process. Greater international collaboration would lead to articulating specific global standards supporting and furthering human rights in technology development. This paper highlights the possible threats to human rights if the legal vacuum is left unattended. The analysis displays a critical juncture between technology and human rights, signifying the need for strategies for filling the present gap. This study adopts descriptive doctrinal legal research methodologies. It highlights the need for internationally coordinated technology governance to ensure that benefits accruing from modern technological developments are harnessed ethically and responsibly and that the human rights of individuals are well protected.

[1]Third Year Student, School of Law, CHRIST University, Bangalore, Email id- pratham.kumar@law.christuniversity.in
[2]Assistant Professor and Co-ordinator, School of Law, CHRIST University, Bangalore, India. shibu.p@christuniversity.in

Key Words: *Emerging Technologies, Cyber Security, Human Rights, Digital Governance, Law and Technology, and Ethical Dilemma.*

1. Introduction

Emerging Technologies refers to modern advancements in various technological domains that might significantly influence the public.[3] They involve a dynamic socio-economic process encompassing both the continuous growth of current technologies and the invention of new ones.[4] In a recent Global survey by Microsoft,[5] it was revealed that around 70% of participants throughout the world were worried about AI-assisted scams.[6] Around 50% of the participants experienced misinformation and disinformation provided to them.[7]

Cybersecurity and emerging technology are closely interlinked. Due to their interconnection, emerging technologies such as artificial intelligence (AI) and the Internet of Things (IoT) increase the surface of cyberattacks, thereby introducing new risks and dangers.[8] Simultaneously, AI and machine learning are being used to develop advanced cybersecurity solutions, making the system more robust.[9] Furthermore, these unregulated technologies leave a higher scope of misuse, indicating a close link with cybersecurity. While technology has become indispensable in our lives and cannot be separated from this society, it positively and negatively impacts human rights[10]. The use of cutting-edge technology aggravates this negative impact, as it undermines traditional ways of holding people accountable for activities that violate human rights since they

[3] Roop L. Mahajan et al., *Cultivating Emerging and Black Swan Technologies*, *in* VOLUME 6: ENERGY, PARTS A AND B 549 (2012), http://doi.org/10.1115/IMECE2012-89339 (last visited Jan 26, 2025).

[4] Samantha Ivett Méndez-Sánchez, *The Work of the Committees in the Business Chambers to Promote the Development of Emerging Technologies*, *in* ADVANCES IN LOGISTICS, OPERATIONS, AND MANAGEMENT SCIENCE 213 (Fernando Ortiz-Rodriguez et al. eds., 2023), http://doi.org/10.4018/978-1-6684-8088-5.ch013 (last visited Jan 26, 2025).

[5] Digital Safety | Global Online Safety Survey Results, https://www.microsoft.com/en-us/DigitalSafety/research/global-online-safety-survey (last visited Jan 26, 2025).

[6] Florian Zandt, Infographic: What Are the Biggest Perceived Dangers of AI?, STATISTA DAILY DATA (2024), https://www.statista.com/chart/32112/most-problematic-ai-scenarios (last visited Jan 26, 2025).

[7] Digital Safety | Global Online Safety Survey Results, *supra* note 3.

[8] Thomas Lange, Houssain Kettani & The Beacom College of Computer and Cyber Sciences, Dakota State University, Madison, South Dakota, USA, *On Security Challenges of Future Technologies*, JCM 1002 (2019).

[9] Willian Dimitrov, *The Impact of the Advanced Technologies over the Cyber Attacks Surface*, 1225 *in* ARTIFICIAL INTELLIGENCE AND BIOINSPIRED COMPUTATIONAL METHODS 509 (Radek Silhavy ed., 2020), https://link.springer.com/10.1007/978-3-030-51971-1_42 (last visited Jan 26, 2025).

[10] Mariam Makanjuola & Cheery Ehimen, *HUMAN RIGHTS AND TECHNOLOGY*, Volume 1 (2024).

make it more challenging to determine accountability for such violations[11]. Due to technology, existing laws are often outdated and cannot effectively prevent human rights violations[12]. These laws are, therefore, compelled to adapt to these changing times, failing which would jeopardize our fundamental rights[13].

The human rights concern is important, owing to these modern technologies' exponential growth and usage[14]. The global AI market is worth around USD 200 billion[15] and is expected to reach USD 1.31 trillion by 2030[16], indicating its widespread everyday use[17]. Modern technologies have grave potential for misuse[18], pointing out that any such action can have devastating consequences on human rights[19]. Further, using emerging technologies in terrorism can harm our fundamental rights[20]. Thus, addressing the implications of such technologies on such rights is paramount.

2. Literature Review

It is of utmost importance to conduct a review of existing literature on a topic in order to avoid repetition of the same work. This paper reviews several research papers on this topic and incidental topics to determine the appropriate scope of the paper.

[11] Humaira Aslam, *Critical Analysis on the Intersection of Technology and Human Rights: Emerging Obstacles to Justice and Accountability"*, 3 AHSS (2022), https://ojs.ahss.org.pk/journal/article/view/310 (last visited Jan 26, 2025).

[12] Vivek Kumar, *The The Intersection of Technology, Privacy, and Human Rights: Judicial Perspectives in India*, 1 MHU INT. JOURNAL OF RES. & INN. 92 (2025).

[13] Lucas E Buckley, Jesse K Fishman & Matthew D Kaufmann, *How Crowdfunding and the On-Demand Economy Are Changing the Legal Field*, https://hkwyolaw.com/the-intersection-of-innovation-and-the-law/ (last visited Jan 26, 2025).

[14] Natalie Runyon, *Human Rights Issues Increasing as Tech Development Rapidly Expands*, THOMSON REUTERS INSTITUTE (2025), https://www.thomsonreuters.com/en-us/posts/human-rights-crimes/human-rights-tech-development/ (last visited Jan 26, 2025)..

[15] GRAND VIEW RESEARCH, *Artificial Intelligence Market Size, Share & Trends Analysis Report By Solution, By Technology (Deep Learning, Machine Learning, NLP, Machine Vision, Generative AI), By Function, By End-Use, By Region, And Segment Forecasts, 2024 - 2030*, https://www.grandviewresearch.com/industry-analysis/artificial-intelligence-ai-market (last visited Jan 26, 2025)

[16] MARKETSANDMARKETS, *Artificial Intelligence (AI) Market*, (2024), https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-market-74851580.html (last visited Jan 26, 2025).

[17] RAYMOND S. T. LEE, ARTIFICIAL INTELLIGENCE IN DAILY LIFE (2020), https://link.springer.com/10.1007/978-981-15-7695-9 (last visited Jan 26, 2025) p.19.

[18] Sarvesh Kumar et al., *Artificial Intelligence: Revolutionizing Cyber Security in the Digital Era*, 2 J. COMPUT. MECH. MANAG 31 (2023).

[19] Onur Bakiner, *The Promises and Challenges of Addressing Artificial Intelligence with Human Rights*, 10 BIG DATA & SOCIETY 20539517231205476 (2023).

[20] Gregory D. Koblentz, *Emerging Technologies and the Future of CBRN Terrorism*, 43 THE WASHINGTON QUARTERLY 177 (2020).

The research paper by Shakleford (2017)[21] examines the relationship between human rights and cybersecurity. However, the article does not depict how specific technological gaps can result in human rights violations. Similarly, the paper by Akyeşilmen (2016)[22]and by Moise (2016), dealing with human rights and cybersecurity, neither analyzes the legal vacuum on emerging technologies nor points out the consequences of the same.

The research paper by M. Roberts (2022)[23] considers technological developments, the importance of cooperation, and the policy gap in modern technology. However, it has not explicitly focused on the legal vacuum surrounding emerging technologies. The paper by Adner and Levinthal (2002)[24] and by Rotelo et. al (2016)[25] have provided the challenges of emerging technology. However, they do not specifically deal with the legal vacuum of these technologies.

Pavlova's (2020)article advocates for a human rights approach to cybersecurity but does not explore the legal gaps in emerging technology or its impacts on specific human rights. Another article by Czuryk (2024)[26] highlights human rights restrictions in the cyber laws of Poland but lacks any discussion on the implications of emerging technologies.

The article by Alvarez-Aros and Erick (2016)[27] and by Veletsianos (2008)[28] highlights the development of emerging technology and its essential elements. However, neither of them

[21] Scott Shackelford, *Human Rights and Cybersecurity Due Diligence: A Comparative Study*, MJLR 859 (2017).

[22] Nezir AkyeşiLmen, *CYBERSECURITY AND HUMAN RIGHTS: NEED FOR A PARADIGM SHIFT?*, 1 (2016).

[23] Megan Roberts, *International Cooperation for a Better Digital Future*, (2022), https://institute.global/insights/tech-and-digitalisation/international-cooperation-better-digital-future (last visited Jan 26, 2025).

[24] Ron Adner & Daniel A. Levinthal, *The Emergence of Emerging Technologies*, 45 CALIFORNIA MANAGEMENT REVIEW 50 (2002).

[25] Daniele Rotolo, Diana Hicks & Ben R. Martin, *What Is an Emerging Technology?*, 44 RESEARCH POLICY 1827 (2015).

[26] Małgorzata Czuryk, *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, 31 SIL 31 (2022).

[27] Erick L. Alvarez-Aros & César A. Bernal-Torres, *Technological Competitiveness and Emerging Technologies in Industry 4.0 and Industry 5.0*, 93 AN. ACAD. BRAS. CIÊNC. e20191290 (2021).

[28] Veletsianos, G., *A Definition of Emerging Technologies for Education. EdTech in the Wild: critical blog posts,* (2019), https://edtechbooks.org/wild/definition_emerging_technologies (last visited Jan 26, 2025).

addresses the ethical concerns of these technologies. The paper by Mordini (2014)[29] lacks a thorough examination of the legal gaps and the broader human rights implications.

The paper authored by Allhoff (2009)[30] highlights the potential risks due to modern technology. The paper by Pariotti (2010)[31] points out the risks due to nanotechnology. Both papers, along with the article by Wilson (2013),[32] highlight the importance of precautionary measures in dealing with such a problem. Through the precautionary principle, the authors showcase the need for cooperation, which is depicted as having a minimal scope. The paper by Kendal (2022)[33] also uses the precautionary principle but does not focus on the legal implications of the gap in emerging technologies or specific human rights violations.

The paper by McGregor and Wetmore (2009)[34] is a narrative review assessing the ethical implications of emerging tech, while the paper by Ashok et. al (2022)[35] is a systematic literature on the legal challenges of AI. The article by Bankins and Formosa (2023)[36] is a literature review on legal gaps in emerging technologies, and that by Hagerty (2019)[37] is a literature review of over 800 sources on AI's social impact. However, none of these articles consider the human rights implications of these legal gaps.

[29] Emilio Mordini, *Considering the Human Implications of New and Emerging Technologies in the Area of Human Security*, 20 SCI ENG ETHICS 617 (2014).

[30] Fritz Allhoff, *Risk, Precaution, and Emerging Technologies*, 3 STUDIES IN ETHICS, LAW, AND TECHNOLOGY (2009), https://www.degruyter.com/document/doi/10.2202/1941-6008.1078/html (last visited Jan 26, 2025).

[31] Elena Pariotti, *Law, Uncertainty and Emerging Technologies: Towards a Constructive Implementationof the Precautionary Principle in the Case of Nanotechnologies*, PERSONA Y DERECHO 15 (2016).

[32] Grant Wilson, *Minimizing Global Catastrophic and Existential Risks from Emerging Technologies Through International Law*, 31 VIRGINIA ENVIRONMENTAL LAW JOURNAL (2012).

[33] Evie Kendal, *Ethical, Legal and Social Implications of Emerging Technology (ELSIET) Symposium*, 19 BIOETHICAL INQUIRY 363 (2022).

[34] Joan McGregor & Jameson M. Wetmore, *Researching and Teaching the Ethics and Social Implications of Emerging Technologies in the Laboratory*, 3 NANOETHICS 17 (2009).

[35] Mona Ashok et al., *Ethical Framework for Artificial Intelligence and Digital Technologies*, 62 INTERNATIONAL JOURNAL OF INFORMATION MANAGEMENT 102433 (2022).

[36] Sarah Bankins & Paul Formosa, *The Ethical Implications of Artificial Intelligence (AI) For Meaningful Work*, 185 J BUS ETHICS 725 (2023).

[37] Alexa Hagerty & Igor Rubinov, *Global AI Ethics: A Review of the Social Impacts and Ethical Implications of Artificial Intelligence*, (2019), http://arxiv.org/abs/1907.07892 (last visited Jan 26, 2025).

Further, the paper by Cozzens et. al (2010)[38] mentions the harms associated with modern technology and uses bibliometric analysis. The article by Carbonell et. al (2017)[39] uses the same method to identify patterns of disseminating emerging technologies on the Internet. The article by Koblentz (2020)[40] provides the risk of emerging tech due to its potential for misuse in terrorism, while the paper by Sechser et. al (2019)[41] highlights the implications of these technologies on war.

The research paper by Wright et. al (2014)[42] highlights the ethical dilemma in emerging tech through scenario construction and stakeholder engagement. However, it is minimal as it only examines the issue in the European context, not the global one. Similarly, the paper by Stahl and Eke (2024)[43] depicts the ethical implications of ChatGPT, while that by Deepika Paira (2020)[44] analyzes the existing legal framework but not the legal implications of the legal vacuum on these emerging technologies.

Upon conducting a thorough review of 26 research papers, two broad research questions may be formulated:

a. What are the legal vacuum's implications on human rights in emerging technologies?
b. What is the scope of the legal vacuum on emerging technologies?
c. What is the role of international organizations in filling the legal vacuum?

The paper aims to address the aforementioned research questions through doctrinal research methodology.

[38] Susan Cozzens et al., *Emerging Technologies: Quantitative Identification and Measurement*, 22 TECHNOLOGY ANALYSIS & STRATEGIC MANAGEMENT 361 (2010).

[39] Javier Carbonell, Antonio Sánchez-Esguevillas & Belén Carro, *Easing the Assessment of Emerging Technologies in Technology Observatories. Findings about Patterns of Dissemination of Emerging Technologies on the Internet*, 30 TECHNOLOGY ANALYSIS & STRATEGIC MANAGEMENT 113 (2018).

[40] Koblentz, *supra* note 19.

[41] Todd S. Sechser, Neil Narang & Caitlin Talmadge, *Emerging Technologies and Strategic Stability in Peacetime, Crisis, and War*, 42 JOURNAL OF STRATEGIC STUDIES 727 (2019).

[42] David Wright et al., *Ethical Dilemma Scenarios and Emerging Technologies*, 87 TECHNOLOGICAL FORECASTING AND SOCIAL CHANGE 325 (2014).

[43] Bernd Carsten Stahl & Damian Eke, *The Ethics of ChatGPT – Exploring the Ethical Issues of an Emerging Technology*, 74 INTERNATIONAL JOURNAL OF INFORMATION MANAGEMENT 102700 (2024).

[44] Deepika Paira, Ensuring Inclusivity in Cybersecurity: A Human Rights Based Approach, CYBER CRIME & CYBER SECURITIES IN INDIA (2023).

3. Emerging Technologies

Emerging Technologies have a rather complex definition. They are those technologies which are evolving tools and innovations that may be new or older, exist in a state of continuous development, undergo hype cycles, and are not yet fully understood or researched[45]. Some popular emerging technologies today are AI, IoT, blockchain, Nanotech, bio-tech, face recognition, etc.[46], which are very few of them in the non-exhaustive list of these technologies.

Artificial intelligence (or AI) is a very commonly used technology today. AI can be defined as the science of endowing programs that can improve themselves due to their own experiences.[47] To put it more simply, AI is the technology that allows computers to simulate human intelligence, learning, problem-solving, creativity, decision making and autonomy.[48]

Another significant technology, the Internet of Things (IoT), is an internet-connected network of physical objects that can communicate with systems and one another.[49] For instance, a few interconnected objects in a household can be considered to be an IoT. Another growing technology is nanotechnology, which deals with materials and processes at a scarcely conceivable smallness measured in billionths of a metre.[50]

An important technological development in today's generation is biotechnology. Utilizing biological systems, living creatures, or their components to develop or produce various outcomes is known as biotechnology.[51] This is majorly observed in genetic engineering. The artificial manipulation, alteration, and recombination of DNA or other nucleic acid molecules to alter an

[45] Veletsianos, G *supra* note 29.

[46] *See* Sahalu Balarabe Junaid et al., *Recent Advancements in Emerging Technologies for Healthcare Management Systems: A Survey*, 10 HEALTHCARE 1940 (2022). *See* also Nikta Shahcheraghi et al., *Nano-Biotechnology, an Applicable Approach for Sustainable Future*, 12 3 BIOTECH 65 (2022).,

[47] Roger C. Schank, *What Is AI, Anyway?*, 8 AIMAG 59 (1987).

[48] Cole Stryker & Eda Kavlakoglu, *What Is Artificial Intelligence (AI)? | IBM*, https://www.ibm.com/think/topics/artificial-intelligence (last visited Jan 26, 2025).

[49] Ricardo Jorge Raimundo & Albérico Travassos Rosário, *Cybersecurity in the Internet of Things in Industrial Management*, 12 APPLIED SCIENCES 1598 (2022).

[50] T. SHELLEY, NANOTECHNOLOGY: NEW PROMISES, NEW DANGERS (2006), https://books.google.co.in/books?id=DnVe7p-N0GAC.

[51] What is Biotechnology at the Department of Biotechnology and Food Science? - NTNU, https://www.ntnu.edu/ibt/about-us/what-is-biotechnology (last visited Jan 26, 2025).

organism or population of organisms is known as genetic engineering.[52] If left unregulated, these emerging technologies would end up as potential hazards to human life. These threats can be better understood theoretically through two prominent theories.

The theory of social construction of technology, also known as SCOT[53], describes that any technological development results from human action[54]. It postulates that technological developments cannot be seen in isolation but must be seen together concerning the social, political, and cultural environment in which they are created[55]. Thus, context plays an important role in understanding technological development[56].

The potential harm due to an emerging technology is fairly visible if seen in a context where it is developed. For instance, during the Covid-19 era, social media was plagued with misinformation and disinformation[57]. The impact of such fake news was rather more destructive. This was due to the role played by AI in promoting the content on the respective platforms, which ensured that the information (though fake) reached the maximum numbers, contributing to millions losing their lives[58].

Furthermore, in the present context, where there exists a legal vacuum on these technologies, the risks of these technologies stand increased. Thus, the legal vacuum ought to be filled at the earliest. The next theory is the right-based approach to technology governance. The right-based approach to technology governance theory postulates that technology must be used and

[52] Genetic engineering | Definition, Process, Uses, Examples, Techniques, & Facts | Britannica, ENCYCLOPEDIA BRITANNICA (2024), https://www.britannica.com/science/genetic-engineering (last visited Jan 26, 2025).

[53] Hans K. Klein & Daniel Lee Kleinman, *The Social Construction of Technology: Structural Considerations*, 27 SCIENCE, TECHNOLOGY, & HUMAN VALUES 28 (2002).

[54] Sara Yousefikhah, *Sociology of Innovation: Social Construction of Technology Perspective*, AD-MINISTER 31 (2017).

[55] Lee Humphreys, *Reframing Social Groups, Closure, and Stabilization in the Social Construction of Technology*, 19 SOCIAL EPISTEMOLOGY 231 (2005).

[56] Odd Einar Olsen & Ole Andreas Engen, *Technological Change as a Trade-off between Social Construction and Technological Paradigms*, 29 TECHNOLOGY IN SOCIETY 456 (2007).

[57] United Nations Human Right Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression: Disease pandemics and the freedom of opinion and expression*, UN Doc. A/HRC/44/49 (2020).

[58] United Nations Human Right Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan: Sustainable development and freedom of expression: why voice matters*, UN Doc. A/HRC/53/25 (2023); Article 19: *International Centre against Censorship, Ensuring the public's right to know in the COVID-19 pandemic*, (2020), https://www.article19.org/resources/ensuring-the-publics-right-to-know-in-the-covid-19-pandemic/ (last visited Jan 26, 2025).

developed in a manner that respects and protectshuman rights. It considers human rights to be the focus of technological development[59]. This approach focuses on creating rights and regulations to protect human rights in the context of technological development, which would provide clear criteria and guidelines for evaluating the impacts of technology on individuals and communities. The approach would highlight the limits of technology, thereby preventing any harm to specific human rights.

4. Human Rights Implications of Emerging Technologies

The UNHRC has noted that people's offline rights must be protected online.[60] Modern technologies have ambivalent impacts on human rights[61], as they can create both positive and negative impacts[62]. Since the positive impacts are majorly undisputed, it is necessary to highlight the adverse effects.

4.1 *Impact on Right to Privacy*

Privacy can be understood as the state of being alone[63] or the assurance that certain information about an entity is kept private and that access to it is restricted.[64] Privacy is a situation with restricted state intervention and the absence of unnecessary intervention by uninvited persons.[65] Right to Privacy is provided under Article 12 of the Universal Declaration of Human Rights

[59] Lisa VeneKlasen et al., *Rights-Based Approaches and beyond : Challenges of Linking Rights and Participation* (2004), https://opendocs.ids.ac.uk/articles/report/Rights-based_approaches_and_beyond_challenges_of_linking_rights_and_participation/26445091.

[60] United Nations Human Right Council, *Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development*, UN Doc.A/HRC/21/L.6 (2012).

[61] Jacopo Coccoli, *The Challenges of New Technologies in the Implementation of Human Rights: An Analysis of Some Critical Issues in the Digital Era*, 1 PEACE HUMAN RIGHTS GOVERNANCE 223 (2017).

[62] Kinfe Yilma, *Emerging Technologies and Human Rights at the United Nations*, 42 IEEE TECHNOL. SOC. MAG. 54 (2023).

[63] Privacy, (2025), https://dictionary.cambridge.org/dictionary/english/privacy (last visited Jan 26, 2025).

[64] CSRC Editor, *Privacy - Glossary | CSRC*, https://csrc.nist.gov/glossary/term/privacy (last visited Jan 26, 2025).

[65] A. LESTER ET AL., HUMAN RIGHTS: LAW AND PRACTICE (2000), https://books.google.co.in/books?id=UjsZAgAACAAJ. para. 4.82. United Nations Human Right Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin*, UN Doc. A/HRC/13/37 (2009) p.11.

(UDHR)and Article 17 of the International Covenant on Civil and Political Rights (ICCPR).[66] In India, several judicial decisions[67] have ruled it to be a part of Article 21 of the Constitution.

In the digital age, the right to privacy extends to both the content of communications and metadata.[68] This is because metadata, when analyzed and aggregated, can reveal information about an individual's behaviour, relationships, preferences, and identity, often exceeding the content's content.[69] In the 21st century, an individual's privacy is a considerable risk.[70] The state, along with businesses operating in the form of applications on the phone, constantly collect data about a person, which may extend but is not limited to their email addresses, phone numbers, biometrics, health and financial data, the majority of which is collected without the person's knowledge or consent.[71]

After this collection, emerging technologies such as AI play a role. They analyze the data obtained from each individual to determine their behavioral patterns and preferences. As per several privacy policies, this data may be disclosed or shared with other third parties[72], thereby blatantly attacking privacy. Even the States use such data. In the recent US Supreme Court

[66] *See* International Covenant on Civil and Political Rights (ICCPR), Dec. 16, 1966

999 U.N.T.S. 171, art. 17. *See also*, African Charter on the Rights and Welfare of the Child art.10; American Convention on Human Rights (ACHR) "Pact of San Jose, Costa Rica", Nov. 22, 1969

1144 U.N.T.S.123, art. 11; Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, Eur. Ts. No. 005, art. 8.

[67] R. Rajagopal vs. State of Tamil Nadu, (1994) 6 SCC 632; K.S. Puttaswamy vs. Union of India AIR 2017 SC 4161; Naz Foundation vs. Govt. of NCT of Delhi 2009 (6) SCC 712; Navtej Singh Johar vs. Union of India 2019 (1) SCC (CRI) 1.

[68] United Nations Human Right Council, *The right to privacy in the digital age Report of the United Nations High Commissioner for Human Rights*, UN Doc. A/HRC/39/29 (2018) p.6.

[69] United Nations Human Right Council, *The right to privacy in the digital age Report of the Office of the United Nations High Commissioner for Human Rights*, A/HRC/27/37 (2014) p.19.

[70] Dhriti Bole, *Right to Privacy in Digital Age*, https://articles.manupatra.com/article-details?id=undefined&ifile=undefined (last visited Jan 26, 2025).

[71] United Nations Human Right Council, supra note 72, at p.12

[72] Data Policy | *Instagram,* https://help.instagram.com/155833707900388 (last visited Jan 26, 2025) Sec. III; Meta Privacy Policy | *Meta,* https://www.facebook.com/privacy/policy/ (last visited Jan 26, 2025), *See* section "*Why and How we process your information" Netmeds Privacy Policy - Safeguarding Your Information*"; *Netmeds,* https://www.netmeds.com/privacy-policy (last visited Jan 26, 2025), cl. 4.3; Privacy Policy | *Tata1mg*, *available at:* https://www.1mg.com/labs/PrivacyPolicy?wpsrc=Google+Organic+Search (last visited Jan 26, 2025) cl. 8B and 8H.

judgement banning Tiktok, the Courts highlighted that the data of 170 million users were being shared with China, as per the requirement of Chinese Laws[73].

The States have been exploiting these emerging technologies by developing systems of secret mass surveillance, claiming it to be necessary for national security. However, the Courts have ruled this practice inconsistent with international law.[74] The States have also developed facial recognition software, which automatically identifies and flags persons.[75] This technology is used by at least half of all federal agencies with law enforcement officers in the US.[76] Even in India, facial recognition technology has grown exponentially in the last 5 years,[77] with Indian authorities spending over Rs.1513 Crore on these technologies.[78] These technologies seriously affect privacy because of their unrestricted use, as they can identify every person in video footage who might not even be an offender.[79] Laws authorizing such vast surveillance contradict the right to privacy[80], as every person does not always consent to surveillance.[81] Article 6 of Convention 108+, which deals with data protection, states that processing special categories of data, such as biometric data, shall only be allowed if there are appropriate safeguards in the domestic law.[82]

[73] Tiktok Inc. v. Merrick B. Garland, 604 U.S. 1 (2025) pg.11.

[74] Roman Zakharov v. Russia, App. no. 47143/06, para. 232. *See* also, United Nations Human Right Council, *Report on best practices and lessons learned on how protecting and promoting human rights contribute to preventing and countering violent extremism Report of the United Nations High Commissioner for Human Rights*, UN Doc. A/HRC/33/29 (2016), para. 58.

[75] United Nations Human Right Council, supra note 72, at p.14.

[76] U. S. Government Accountability Office, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Have Better Awareness of Systems Used By Employees | U.S. GAO*, https://www.gao.gov/products/gao-21-105309 (last visited Jan 26, 2025).

[77] Amber Sinha, *The Landscape of Facial Recognition Technologies in India | TechPolicy.Press*, https://www.techpolicy.press/the-landscape-of-facial-recognition-technologies-in-india/ (last visited Jan 26, 2025).

[78] Jayant Pankaj, *Widespread use of facial recognition tech across India - The Hindu BusinessLine*, https://www.thehindubusinessline.com/data-stories/amid-growing-need-for-security-over-1513-crore-invested-in-deploying-facial-recognition-technology-across-country/article68288599.ece (last visited Jan 26, 2025).

[79] Jake Laperruque, *Limiting Face Recognition Surveillance: Progress and Paths Forward*, CENTER FOR DEMOCRACY AND TECHNOLOGY (Aug. 23, 2022), https://cdt.org/insights/limiting-face-recognition-surveillance-progress-and-paths-forward/ (last visited Jan 26, 2025).

[80] CoE, *Declaration of the Committee of Ministers of the Council of Europe on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies*, (adopted on 11 June 2013), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168068460d (last visited Jan 26, 2025).

[81] CoE, *Guidelines on Facial Recognition*, https://rm.coe.int/guidelines-facial-recognition-web-a5-2750-3427-6868-1/1680a31751 ((last visited Jan 26, 2025).

[82] CoE, *Convention 108+: Convention for the protection of individuals with regard to the processing of personal data*, (adopted on 18 May, 2018), art. 6.

However, this surveillance, being mainly secretive, does not allow people to know about it, thus contravening the convention.

4.2 *Impact on Freedom of Expression*

Freedom of Expression is guaranteed to everyone under Article 10 of the UDHR, Article 19 of the ICCPR and Article 19(1)(a) of the Indian Constitution,[83] along with several other conventions.[84] It is recognized to be indispensable in every democratic society.[85] Through these emerging technologies, a negative impact is caused on free speech. The government makes several laws relating to sedition defamation, which limit the exercise of free speech. The government may also make such laws to silence criticism,[86] ultimately weakening democracy in the country.[87]

Regardless, social media platforms ought to comply with these laws by removing content on their platforms, which is against the law. However, it is impractical for platforms such as YouTube to

[83] UDHR, *supra* note 69, at art.10; ICCPR, *supra* note 70, at art. 19; INDIA CONST. art. 19, § 1, cl. a.

[84] European Convention on Human Rights ('ECHR') (adopted 4 November 1950, entered into force 3 September 1953) 213 UNTS 1932 art 10; ACHR, *supra* note 69, at art.13; African Charter on Human and Peoples' Rights (AChHPR) (adopted 27 June 1981, entered into force 21 October 1986) 21 ILM 58 art 9; Arab Charter on Human Rights (adopted 22 March 2004, entered into force 15 March 2008), arts. 32; ASEAN Declaration on Human Rights (adopted 9 November 2012), arts. 23.

[85] Handyside v United Kingdom, App no 5493/72 para.49; Bowman v United Kingdom App no 24839/94 para. 42; Tae Hoon Park v Republic of Korea, CCPR/C/64/D/628/1995 para. 10.3; Perna v Italy, App no 48898/99 para. 39; Steel and Morris v the United Kingdom, App no 68416/01 para. 87; Vladimir Viktorovich Shchetko v Belarus, CCPR/C/87/D/1009/2001 para. 7.3; Stephen Benhadj v Algeria CCPR/C/90/D/1173/2003 para. 8.10; Zhagiparov v Kazakhstan, CCPR/C/124/D/2441/2014 para. 13.3.

[86] United Nations Human Right Council, *Interim report of the Special Rapporteur on freedom of religion or belief,* UN Doc A/65/207 (2010); OHCHR, *Annual Report of High Commissioner for Human Rights 2010* (2011); Smith, James Morton, *The Sedition Law, Free Speech, and the American Political Process,* WILLIAM AND MARY QUARTERLY, 9 (1952); Brian Bond, *"Criticism is Not a Crime" – High Commissioner for Human Rights*, EDMUND RICE INTERNATIONAL, (2010).

[87] William T. Mayton, *Seditious Libel and the Lost Guarantee of a Freedom of Expression*, 84 COLUMBIA LAW REVIEW 91 (1984). Arudra Burra, *'Review of 'Sedition in Liberal Democracies' by Anushka Singh,* 15 SLR 66 (2019); Vineet Pratap Singh, *The Correlation of the Right to Dissent and Sedition* 4IJLLR (2022).

manually review 400 hours of videos uploaded by its users per minute.[88] Thus, they resort to using AI to monitor the content and remove it if a violation of the law is found.[89]

Social media platforms are often penalized heavily for failure to remove content that violates the provisions of law and causes disturbance of peace or tranquillity. Thus, to be safer, they end up over-criminalizing content (i.e., over-censorship), ultimately restricting lawful speech.[90] Furthermore, these platforms, being ill-equipped to determine the illegality of content,set the threshold low in their respective community guidelines, allowing AI to remove content, even if the content would be completely legal. This lack of human review for such content would severely undermine freedom of expression due to the delegation of the decision-making power to AI alone.

4.3 *Impact on the Security of Individuals*

Article 3 of the UDHR guarantees everyone a right to security of person, which is also guaranteed under Article 9 of the ICCPR[91]. This right requires the state to protect a person's physical and mental security.[92] This right ensures the persons enjoying it have a sense of security from arbitrary interference[93]. However, this right has not yet been able to provide such protection to individuals. The cost of cybercrimes in 2020 was almost 1% of the Global GDP[94]. With the development of modern technologies, individuals' security is greatly diminished.

---

[88] Daphne Keller, *The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation* (2018), https://lawcat.berkeley.edu/record/1128543 (last visited Jan 26, 2025).

[89] How Instagram uses artificial intelligence to moderate content | Instagram Help Center, https://help.instagram.com/423837189385631 (last visited Jan 26, 2025).

[90] United Nations Human Right Council, *Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, A/HRC/23/40 (2013) para.49; David Ingram, *Foreign Governments Are Fed up with Social Media — and Threatening Prison for Tech Employees*, https://www.nbcnews.com/tech/tech-news/foreign-governments-are-fed-social-media-threatening-prison-tech-employees-n993841 (last visited Jan 26, 2025). Luís Roberto Barroso, Luna van Brussel Barroso *Democracy, Social Media, and Freedom of Expression: Hate, Lies, and the Search for the Possible Truth* 24 Chic. J. Int. Law 51 (2023).

[91] UDHR, *supra* note 69, at art.3; ICCPR, *supra* note 70, at art.9, CRPD, *supra* note 69, at art. 14.

[92] Canadian Charter of Rights and Freedoms, 1982, s.7, Part 1 of the Constitution Act, 1982 (Canada); The Protection of Human Rights (Amendment) Act, 2019, s. 29, No. 19 of 2019, Acts of Parliament, 2019 (Queensland).

[93] Rhonda Powell, *The Legal Right to Security of Person*, *in* RIGHTS AS SECURITY 10 (1 ed. 2019), https://academic.oup.com/book/35225/chapter/299741882 (last visited Jan 26, 2025).

[94] Frank Cremer et al., *Cyber Risk and Cybersecurity: A Systematic Review of Data Availability*, 47 GENEVA PAP RISK INSUR ISSUES PRACT 698 (2022).

The Internet of Things (IoT) is an interconnected system of objects that compromises security. This is because if one device in the system is hacked, the system collapses, and a third party can easily control the system with physical access.[95] Furthermore, many such networks operate in unattended environments, making the network susceptible to various threats, such as eavesdroppingor flooding of systems with corrupted messages that leave them unfit for use.[96] This severely impacts the security of individuals.

The next issue affecting people's security is data theft. Since 2000, the personal information of around 3.5 billion people has been stolen, constituting almost half the world's population.[97] Furthermore, in 2024, the National Public Data leak in the US leaked data of 2.9 billion people,which was later published on the dark web around April 8, 2024, by a cybercriminal group, USDoD.[98] Moreover, certain apps with over 10 lakh downloads were found to have been sharing data with malicious actors in China.[99] As mentioned earlier, many other apps, such as social media platforms and e-pharmacies, have also been sharing user data with third parties, all of which ultimately jeopardize this right to security, and the States have failed to fully guarantee this right to the individuals.

[95] Tinshu Sasi et al., *A Comprehensive Survey on IoT Attacks: Taxonomy, Detection Mechanisms and Challenges*, 2 JOURNAL OF INFORMATION AND INTELLIGENCE 455 (2024).

[96] Nataliia Neshenko et al., *Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations*, 21 IEEE COMMUN. SURV. TUTORIALS 2702 (2019).

[97] Mounika Mandapuram, *Application of Artificial Intelligence in Contemporary Business: An Analysis for Content Management System Optimization*, 7 ASIAN BUS. REV. 117 (2017).

[98] Jennifer Gregory, *National Public Data Breach Publishes Private Data of 2.9B U.S. Citizens*, https://securityintelligence.com/news/national-public-data-breach-publishes-private-data-billions-us-citizens/ (last visited Jan 26, 2025).

[99] Abhik Sengupta, *Android Apps with over 10 Lakh Downloads Found with Spyware Sending Data to China - India Today*, https://www.indiatoday.in/technology/news/story/android-apps-10-lakh-downloads-found-spyware-sending-data-china-2404247-2023-07-10 (last visited Jan 26, 2025).

4.4 *Impact on Right to Life*

The right to life, one of the most basic fundamental rights, is guaranteed to everyone under Article 21 of the Indian Constitution.[100] It is also granted to us under Article 3 of UDHR and Article 6 of the ICCPR.[101] In this era of emerging technologies, this right to life is also at stake. A rapidly growing technology known as Nanotechnology deals with materials and processes at a conceivable smallness measured in billionths of a metre.[102] Though it has many advantages, it also brings many dangers.[103] Nanomaterials can exhibit unusual reactions due to manipulation at the nanoscale, posing unique health risks and hazards.[104] Nanotechnology can be used for easier entry into the body or the cells in the body, which is commonly used in medicine.[105] However, along with advancements in genetics, nanotechnology might make it possible for chemical and biological weapons to react selectively to specific gene patterns or proteins, which could have disastrous consequences.[106] Such a technology is very likely to cause genocide.

Genocide, as per the Genocide Convention, is any act committed with the intent to destroy, in whole or in part, a national, ethnical, racial, or religious group, including killing its members, causing serious harm, inflicting conditions to bring about its destruction, preventing births, or forcibly transferring children.[107] For instance, if the technology is targeted at specific genetic or biological traits which are associated with particular ethnic or racial groups, then it could end up in ethnic cleansing of that target population, resulting in the crime of genocide.

The US, in the race for modern technologies, under the 21st Century Nanotechnology Research and Development Act, allocated $849 million to the development of nanotechnology.[108] In 2024,

[100] INDIA CONST., art. 21.

[101] UDHR, *supra* note 69, at art.3, ICCPR, *supra* note 70, at art.6.

[102] SHELLEY, *supra* note 51.

[103] European Union, *Nanotechnologies*, https://ec.europa.eu/health/scientific_committees/opinions_layman/en/nanotechnologies/l-2/6-health-effects-nanoparticles.htm (last visited Jan 26, 2025).

[104] Andrew Maynard, *Nanotechnology: The Next Big Thing, or Much Ado about Nothing?*, THE ANNALS OF OCCUPATIONAL HYGIENE (2006), https://academic.oup.com/annweh/article/51/1/1/173801/Nanotechnology-The-Next-Big-Thing-or-Much-Ado (last visited Jan 26, 2025).

[105] Abid Haleem et al., *Applications of Nanotechnology in Medical Field: A Brief Review*, 7 GLOBAL HEALTH JOURNAL 70 (2023).

[106] Jürgen Altmann, *Military Uses of Nanotechnology: Perspectives and Concerns*, 35 SECURITY DIALOGUE 61 (2004).

[107] Convention on the Prevention and Punishment of the Crime of Genocide, Dec. 9 1948, S. Exec. Doc. O, 81-1 (1949), 78 U.N.T.S. 277, art. 2.

[108] Whitehouse Geroge w Bush, *President Bush Signs Nanotechnology Research and Development Act*, https://georgewbush-whitehouse.archives.gov/news/releases/2003/12/20031203-7.html (last visited Jan 26, 2025).

the US requested an exorbitant sum of $2.16 Billion for the National Nanotechnology Initiative.[109] The scheme has already generated $43 Billion since its formation in 2001.[110] Thus, with the rapid development of these technologies, the right to life is put in grave danger despite the probable benefits of such technology.

Another factor adversely affecting the livelihood of specific sectors of people is caused due to AI. Social media platforms use AI algorithms to display content to the user.[111] In doing so, AI would depict engaging content, which leads to amplified popular narratives on a topic. If the views of marginalized communities go against the popular narratives and are not engaging enough, their content might not be depicted sufficiently, and their views might be suppressed.

eaningful engagement of poor and marginalized communities is essential for good development.[112] The state must create an environment where such communities can freely express their views.[113] Giving voice to such communities is essential for their development.[114] However, with AI operating in a contrary manner, marginalized communities cannot be expected to develop and will remain disadvantaged, indirectly affecting their life and livelihoods. Furthermore, generative AI has promoted misinformationand disinformation several times and continues to do so inadvertently.[115] False information of such nature can reinforce negative opinions about marginalized communities, again exacerbating their disadvantaged position and affecting their life adversely. For instance, AI has been used to spread false information, such as those that claim that Haitian Americans are eating pets or that illegal immigrants into the US are voting illegally without any proper document.[116] Such information targets such communities,

[109] Lynn L. Bergeson & Carla N. Hutton, *NNI Publishes Supplement to the President's 2024 Budget Request*, BERGESON & CAMPBELL, P.C. (2024), https://www.lawbc.com/nni-publishes-supplement-to-the-presidents-2024-budget-request/ (last visited Jan 26, 2025).

[110] National Nanotechnology Initiative, *NNI Supplement to the President's 2024 Budget* (March 05, 2024).

[111] Scott M. Graffius, How Algorithms Shape the User Experience on Social Media Platforms, https://scottgraffius.com/blog/files/tag-how-algorithms-shape-the-user-experience-on-social-media-platforms.html (last visited Jan 26, 2025).

[112] Bridget Pratt, *Inclusion of Marginalized Groups and Communities in Global Health Research Priority-Setting*, 14 JOURNAL OF EMPIRICAL RESEARCH ON HUMAN RESEARCH ETHICS 169 (2019).

[113] United Nations Human Right Council, *supra* note 59.

[114] Pooja Bachani, *Engaging Marginalized Communities: Challenges and Best Practices | Icma.Org*, https://icma.org/articles/pm-magazine/engaging-marginalized-communities-challenges-and-best-practices (last visited Jan 26, 2025).

[115] Tate Ryan-Mosley, *How Generative AI Is Boosting the Spread of Disinformation and Propaganda | MIT Technology Review*, https://www.technologyreview.com/2023/10/04/1080801/generative-ai-boosting-disinformation-and-propaganda-freedom-house/ (last visited Jan 26, 2025).

[116] Samuel Woolley, *To Overcome AI-Enabled Propaganda, Support Communities Already Fighting It*, CENTRE FOR INTERNATIONAL GOVERNANCE INNOVATION, https://www.cigionline.org/articles/to-overcome-ai-enabled-propaganda-support-communities-already-fighting-it/ (last visited Jan 26, 2025).

exploiting their fears and enhancing inequality more effectively. Even in India, fake news has created enormous problems for these communities. In the Manipur conflict, two women were paraded naked after a fake picture of a tribal person's murder was circulated in the Imphal Valley.[117] Fake news being circulated on social media increased tensions between the two communities, leading to the commission of violent and merciless acts against the disadvantaged communities.[118] Thus, the right to life is also at peril with the evolution of emerging technologies.

5. Legal Vacuum On Emerging Technologies

Emerging technologies are growing at an extremely rapid pace. Researchers have discovered that in the last 250 years, scientific journals have doubled every 15 years, while important discoveries have doubled every 20 years.[119] Such is the speed of technology. However, legislation and laws for potential oversight of these technologies are slowing down.[120]

This US Office of Technology Assessment noted several years ago that technological changes, which were once very slow, are now outpacing the legal system that governs it.[121] The surge in AI usage happened in 2012, especially around 2020, when OpenAI started testing GPT-3,[122] which was later made free and accessible to all. However, AI is governed primarily by the Information Technology Act 2000,[123] enacted almost 20 years before the widespread use of AI. Furthermore, no dedicated legislation relating to AI or any other emerging technology exists in Indi. Even nanotechnology, bits and pieces, are governed by different laws without one specific

[117] Manipur violence: How fake news and videos inciting violence in Manipur - The Economic Times, https://economictimes.indiatimes.com/news/india/how-fake-news-and-videos-inciting-violence-in-manipur/articleshow/102065845.cms?from=mdr (last visited Jan 26, 2025).

[118] *See* Shruti Menon, *Manipur: Misleading Information Shared about India Tensions*, https://www.bbc.com/news/world-asia-india-66255989 (last visited Jan 26, 2025).

[119] Derek J. De Solla Price, LITTLE SCIENCE, BIG SCIENCE (1963), https://www.degruyter.com/document/doi/10.7312/pric91844/html (last visited Jan 26, 2025).*See also* Ilkka Tuomi, *Kurzweil, Moore, and Accelerating Change* (2003)..

[120] Gary E. Marchant, *The Growing Gap Between Emerging Technologies and the Law*, 7 *in* THE GROWING GAP BETWEEN EMERGING TECHNOLOGIES AND LEGAL-ETHICAL OVERSIGHT 19 (Gary E. Marchant, Braden R. Allenby, & Joseph R. Herkert eds., 2011), https://link.springer.com/10.1007/978-94-007-1356-7_2 (last visited Jan 26, 2025)..

[121] U.S. Congress, Office of Technology Assessment, *Intellectual Property Rights in an Age of Electronics and Information*, OTA-CIT-302, Washington, DC: U.S. Government Printing office (1986).

[122] What is the history of artificial intelligence (AI)? | Tableau, https://www.tableau.com/data-insights/ai/history (last visited Jan 26, 2025).

[123] Information Technology Act, 2000, No. 21 of 2000, Acts of Parliament (India).

law.[124] Due to the lacunae in governing emerging technology in the country's domestic legal system, international conventions and agreements must be resorted to.

On the International level, there exists the Convention on Cybercrime or the Budapest Convention, which came into effect on July 1, 2004.[125] The Preamble to the Convention provides that the convention aims to deter actions against computer systems and networks.[126] It ensures the prevention of cybercrimes by making domestic laws on the matter.[127] Being an old convention, it lacks in its application to emerging technologies. It does not consider issues related to cloud computing, as cloud services lead to jurisdictional and legal challenges. It does not address the role of AI in AI-driven attacks and deepfakes. In other words, the convention is ineffective and does not address modern challenges.

A recent development in this area is the adoption of a new Cybercrime Convention. The UN General Assembly adopted the United Nations Convention Against Cybercrime on 24 December 2024.[128] The convention aims to establish rules to prosecute cybercriminals and foster international cooperation between countries in investigations and exchanging electronic evidence. The convention lays down certain safeguards to secure human data and privacy. The convention touches upon emerging technologies as well, but not directly. It incidentally regulates crimes facilitated by such technology, such as hacking into smart devices or exploiting vulnerabilities in the Internet of Things (IoT). However, the convention does not address all forms of cybercrimes relating to emerging technologies, such as blockchain, AI or quantum computing. It does not delve deeply into the challenges produced by each of these technologies, which could result in one-size-fits-all approaches to all the technologies, which would not be very effective.

[124] *See* Ritika Kumari et al., *Regulation and Safety Measures for Nanotechnology-Based Agri-Products*, 5 FRONT. GENOME ED. 1200987 (2023); *See also* MD KARIM, NANOTECHNOLOGY LAW AND POLICY: AN INTRODUCTION (2013).

[125] CoE, Convention on cybercrime, (adopted in 2011), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:4656911 (last visited Jan 26, 2025).

[126] CoE, Convention on Cybercrime (2011), Preamble.

[127] Budapest Convention - Cybercrime, https://www.coe.int/en/web/cybercrime/the-budapest-convention (last visited Jan 26, 2025).

[128] United Nations Convention against Cybercrime, UNITED NATIONS : OFFICE ON DRUGS AND CRIME, //www.unodc.org/unodc/en/cybercrime/convention/home.html (last visited Jan 26, 2025).

Primarily, the convention addresses criminal activities rather than regulatory or ethical concerns surrounding emerging technologies.

Thus, no effective international treaty or convention completely regulates emerging technologies.[129] This creates enormous problems as no appropriate penalty is prescribed for those who misuse these technologies. If any wrong is committed due to AI, there is ambiguity in defining who is attributable to such wrong. Again, there is a challenge in cases of deep-fakes generated by AI as there is no framework to ascertain liability, while such deep-fakes can spread misinformation and ruin honour and reputation.[130] Furthermore, criminals may identify flaws in AI algorithms to steal and misuse data.[131] Further, if AI commits a mistake due to negligence, it is unclear who is liable for it.[132] The existing and recent conventions are silent on these issues. Thus, there exists a significant legal vacuum in these technologies, with the Conventions addressing a tiny portion of this legal and ethical issue, which must be addressed soon.

6. The Role of International Organizations

International organizations such as the United Nations, NATO, EU, and ASEAN play a significant role in filling the legal gap in emerging technologies.

6.1 *United Nations Organization*

To resolve this legal vacuum on emerging technologies, there have been no instances in the past. However, the Secretary General of the United Nations has recognised a significant gap in international cooperation on artificial intelligence, thus aiming to achieve cooperation on this issue.[133] On 18th July 2023, the first formal meeting on the emerging technology of AI was held in the Security Council.[134] In order to fulfil the 2030 agenda, the UN Secretary-General has made

[129] Digital Regulation Platform, https://digitalregulation.org (last visited Jan 26, 2025).

[130] TODD C. HELMUS, ARTIFICIAL INTELLIGENCE, DEEPFAKES, AND DISINFORMATION: A PRIMER (2022), https://www.rand.org/pubs/perspectives/PEA1043-1.html (last visited Jan 26, 2025).

[131] Hifajatali Sayyed, *Artificial Intelligence and Criminal Liability in India: Exploring Legal Implications and Challenges*, 10 COGENT SOCIAL SCIENCES 2343195 (2024).

[132] *Id.*

[133] UN, Report of the Secretary-General: Roadmap for Digital Cooperation (June 2020), https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf ((last visited Jan 26, 2025).

[134] International Community Must Urgently Confront New Reality of Generative, Artificial Intelligence, Speakers Stress as Security Council Debates Risks, Rewards | Meetings Coverage and Press Releases, https://press.un.org/en/2023/sc15359.doc.htm (last visited Jan 26, 2025).

four commitments about emerging technologies. These are to (a) Boost the UN's internal capacities and use of these technologies, (b) Promote understanding and discussion about emerging technologies; (c) Support talks on rules and collaboration for these technologies; and (d) Help governments build their capacity in these areas.[135]

6.2 *NATO*

NATO (or the North Atlantic Treaty Organization), in order to direct their efforts to promote the development of emerging technologies and provide a platform to assist allies in defending themselves against threats associated with such technologies, NATO developed a strategy in February 2021 known as "Foster and Protect: NATO's Coherent Implementation Strategy on Emerging and Disruptive Technologies."[136] NATO established the Defence Innovation Accelerator for the North Atlantic (DIANA) in 2021 to promote collaboration among allies on emerging technologies and work closely with academia and the private sector through start-ups and venture capital funds to achieve the highest level of innovation in this area.[137] They have also established a EUR 1 billion venture capital fund named the "NATO Innovation Fund" (NIF) to provide investments in start-ups for these technologies to its 24 NATO allies.[138] The world's first AI Strategy, which addresses the responsible military use of AI, was adopted by NATO foreign defence ministers.[139] In order to support allied quantum technology ecosystems, NATO also maintains a "Transatlantic Quantum Community", which was officially launched on 2nd July 2024, where allies exchange technical knowledge and experience on quantum technology, which is again a leading emerging technology today.[140]

[135] The Secretary-General's Strategy on New Technologies | United Nations, https://www.un.org/en/un-chronicle/secretary-general%E2%80%99s-strategy-new-technologies-0 (last visited Jan 26, 2025).

[136] Raluca Csernatoni & Bruno Oliveira Martins, *Disruptive Technologies for Security and Defence: Temporality, Performativity and Imagination*, 29 GEOPOLITICS 849 (2024).

[137] Raquel Jorge Ricart, *NATO Defence Innovation and Deep Tech: Measuring Willingness and Effectiveness* (2023).

[138] The Nato Innovation Fund | NIF, NATO INNOVATION FUND, https://www.nif.fund/ (last visited Jan 26, 2025).

[139] Soare Simona R, *Algorithmic power, NATO and artificial intelligence*, IISS, https://www.iiss.org/ja-JP/online-analysis/military-balance/2021/11/algorithmic-power-nato-and-artificial-intelligence/ (last visited Jan 26, 2025).

[140] AGENCE EUROPE - Transatlantic Quantum Community held its inaugural meeting..., https://agenceurope.eu/en/bulletin/article/13445/33 (last visited Jan 26, 2025).

6.3 *Other International Organizations*

The European Union was the first to create a legally binding international instrument on cybercrime, known as the Budapest Convention.[141] According to Article 23 of the Convention, the parties must collaborate as much as practicable on any investigations or processes of cybercrimes.[142] Even though the convention only covers cooperation for proceedings or investigations, it also acknowledges the necessity of working together to counter cybercrimes or the abuse of modern technology for such purposes. The ASEAN (or the Association of South-East Asian Nations) has successfully developed a guide on AI Governance and Ethics that organisations may use to create and develop AI technologies for non-military or commercial uses.[143] Additionally, acknowledging the possible ramifications of AI, ASEAN held a ministerial meeting stressing the necessity of cooperation on AI.[144]

7. Conclusion and Recommendations

Emerging Technologies is a rapidly evolving field of technological innovation that has seen widespread usage in the 21st century. With all the benefits it comes up with, there are several negative issues which, if left unchecked, can cause devastating impacts on humans. This indicates that this field is very sensitive and must be treated with the utmost care.

These technologies potentially impact privacy, freedom of expression, security of individuals, and right to life, among other human rights. These rights are some of the basic human rights, and they must be safeguarded at all costs. The States can protect such rights by taking a human rights-centric approach towards technological innovations. By making human rights the primary concern, these technologies can be regulated accordingly through laws and policies to safeguard these rights while incentivizing technological developments effectively. The existing domestic legal framework is outdated and cannot adapt adequately to these technologies' modern challenges. The laws were created at a point when such technologies were still in the developing

[141] Budapest Convention - Cybercrime, *supra* note 135.

[142] *Id.* at art. 23

[143] ASEAN, *ASEAN Guide on AI Governance and Ethics*, https://asean.org/book/asean-guide-on-ai-governance-and-ethics/ (last visited Jan 26, 2025).

[144] ASEAN Ministerial Meeting on Science, Technology and Innovation (AMMSTI) Statement on Artificial Intelligence (AI) - ASEAN Main Portal, https://asean.org/asean-ministerial-meeting-on-science-technology-and-innovation-ammsti-statement-on-artificial-intelligence-ai/ (last visited Jan 26, 2025).

stage. Thus, they are not applicable effectively in the modern age. Technologies will keep evolving, indicating that we require laws to adjust to new challenges and effectively tackle them.

In the global arena, it is appreciated that the UN has taken the initiative to tackle cybercrime by laying down a new convention. The convention incidentally touches upon the issues due to emerging technologies but does not entirely resolve them. Thus, in the absence of any convention which can completely regulate emerging technologies, a significant portion of the legal vacuum is left unfilled. International organizations have taken individual approaches to tackle the issues owing to emerging technologies and have been successful in their approach. However, instead of individual developments, if all 193 member countries of the UN cooperate to address this problem, the result would effectively resolve all issues, leading to a robust system to protect the human rights of every individual on Earth.

Thus, it is recommended that multilateral cooperation happens globally and that the UN develop an international instrument addressing emerging technologies specifically. States that ratify the convention must make laws to address this issue in their respective legal system. The convention must require all States to take a human rights-centric approach while making any technological innovation and be required to develop policies that incentivize innovation without compromising human rights. Engaging with diverse stakeholders, such as tech companies, civil society and academia, in decision-making will result in more inclusive and effective solutions.

At the domestic level, it is recommended that the States develop new laws to address modern technologies and human rights concerns. If the States are not in a position to make new laws, the bare minimum required from them is to make amendments to the existing laws so that these technologies are brought into the scope of such laws. For instance, the Information Technology Act 2000 must be amended to include the definition of AI in the legislation and prescribe the appropriate penalty for those who misuse AI, such as creating deepfakes and circulating it. Only with legislative interference can human rights be effectively protected in the modern age of technology.