Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal – The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi, Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

SECURING PRIVACY IN THE ERA OF COMPUTER VISION

AUTHORED BY - SRINITHI. V & SANCHITA. S

1. INTRODUCTION:

A Human Eye while observing the outside world not only uses vision but also synergizes the personal experience and the abstract concept of the thing to augment the perspective of our daily life. In the same way an Artificial Intelligence has been developed within a limited scope of the Visual abilities of a Human Species. Therefore, Computer vision is a contemporary branch of computer science that focuses on aspects of the complexity of the human visual system to make it possible for computers to recognize and analyze things in photos and videos in a manner similar to that of humans. The Convergence of computer vision technologies with artificial intelligence and big data processing has unlocked a multitude of possibilities, ranging from personalized marketing to smart surveillance systems. However, these unprecedented capabilities raise concern about how personal information is collected, used and stored, necessitating the implementation of robust privacy and data protection measures.

1.1. WHAT IS COMPUTER VISION AND HOW IT WORKS:

Computer vision is the application of Artificial intelligence's image recognition model by enabling computers to use digital images and deep learning models to precisely recognise, categorise and respond to object.   By extracting visual input, analyzing it, and evaluating the results, computer vision aims to teach computers how to read and comprehend images on a pixel-by-pixel basis. Convolutional neural networks (CNN) and deep learning, a particular type of machine learning, are the two main methods employed to do this.

With the help of pre-programmed algorithmic frameworks, a machine learning system may automatically learn about the interpretation of visual data. If the model is given a sizable enough dataset, it can learn to differentiate between similar images. This in turn substitute human labour in activities like picture recognition with algorithms by enabling the system to learn on its own.

Convolutional neural networks help deep learning and machine learning models understand by breaking up images into smaller, taggable portions. It executes convolutions with the aid of the tags and then uses the tertiary function to gain insight into the scene it is watching. The neural network conducts convolutions during each cycle and assesses the accuracy of its recommendations. And that's when it starts perceiving and identifying pictures like a human.

1.2. COMPUTER VISION AND ITS HISTORY:

As it was

Early computer vision research in the 1960s focused mostly on developing algorithms that could recognise simple shapes and edges in images. In order to do this, rules and heuristics had to be manually entered into the computer, which then used a method known as "edge detection" to discover edges and lines in the photos. Technically speaking, this suggests that the foundation of image analysis is made up of straight lines and other simple forms since they were discovered to be highly sensitive to sharp edges and lines.

In 1970s – The National Bureau of Standards scientist Kirsch scanned a picture of his small child into a computer more than 50 years ago, this first digital image was a hazy, black-and-white photograph of a baby that changed the way we perceive the world. Ever since the use of neural networks to improve the accuracy of computer vision algorithms has been studied. Neural networks, a type of machine learning that mimics how the human brain processes information, allow computers to learn from enormous datasets. As a result, computers can improve over time.

In 1980s - One of the most important developments in computer vision occurred when scientists created the Hough Transform, a mathematical algorithm that could recognise intricate forms in images. Through the use of lines, circles, and other geometric shapes, the Hough Transform made it possible to discern between objects in images.

During the 1990s and the early 2000s, computer vision continued to evolve as researchers developed ever-more complicated techniques for object identification, facial recognition, and image recognition. As a result, effective computer vision algorithms that could recognise objects in real time and under difficult circumstances were developed.

As it exists:

Artificial intelligence has significantly changed computer vision since it enables machines to perceive and analyse visual input unlike ever before. Convolutional neural networks (CNNs), one type of deep learning method, have proven particularly useful in computer vision. Computers can now recognise objects and patterns in photos with remarkable accuracy thanks to CNNs, which are designed to imitate the structure of the human visual system. Applications have greatly improved as a result, including image identification, object detection, and facial recognition. Since its inception, computer vision has come a long way, and it is now an essential technology in many industries, such as manufacturing, security monitoring, robotics, augmented reality, and health care.

Future Vision:

The way we interact with the world around us is about to change as computer vision advances. Due to advancements in deep learning, artificial intelligence, and specialised hardware, computer vision has a promising future. One of the most important areas for growth in computer vision (AR) is the field of augmented reality. Computers can overlay digital information on the real world using augmented reality (AR) technology, which enhances our perception of reality. Through the use of computer vision algorithms, AR apps can identify and track objects in the real world, enabling the seamless integration of digital content into daily life. From gaming to education, augmented reality has the potential to transform a variety of industries. The future of computer vision is bright with advances in deep learning, artificial intelligence, and specialised hardware creating new prospects for many industries.

1.3.RESEARCH PROBLEM:

As computer vision system become more advanced and pervasive, they have the potential to capture and process visual data without user's explicit consent or awareness. This situation creates new challenges, which need to be addressed to ensure securing privacy in the era of computer vision. This Research aims to probe into the implication of data protection and privacy in the context of Computer Vision Technology in India. It explores the potential ethical implications that arise when using computer vision technologies and highlight the importance of establishing clear framework and guidelines. It emphasizes the technological advancement and the individual autonomy, urging the developers and policymakers to work hand in hand to ensure responsible use of computer vision

system.

1.4. <u>LITERATURE REVIEW:</u>

2. In Defence of Ethics *and* the Law in AI Governance: The Case of Computer Vision - https://link.springer.com/chapter/10.1007/978-3-031-19149-7_5

This particular research has been published by Palgrave Macmillan, Cham ISBN- 978-3-031-19148-0, This journal mainly focuses on the ethical compliance of the AI system in the domain of R&D, offering insight into various harms of AI and awareness of the same. This paper also deals with how the world has gone from "raise in AI" to "rush to Governance of AI". In a case study of the legal and ethical evaluation of access, collection, and other sorts of processing of personal data for the purpose of computer vision, it narrows the focus on the relationship between ethics and law. It demonstrates how, while there are contradictions between ethics and the law, they are complimentary in preventing the possible detrimental societal and personal effects of AI.

3. The Ethics of computer Vision: an overview in terms of power- https://link.springer.com/article/10.1007/s43681-023-00272-x

This Research done by Rosalie. A. Waelen with DOI: https://doi.org/10.1007/s43681-023-00272-x, specifically focuses on the ethics of computer vision and its impact on the value of autonomy and the normative goal of emancipatory progress. The author creates an overview of ethical, social, and political issues related to computer vision, using a critical approach. The focus of the analysis was predominantly on those CV applications that involve the analysis of persons. A limitation of this approach is that it does not necessarily offer guidance in determining how severe an application's impact on autonomy will really be.

4. Will India's Proposed Data Protection Law Protect Privacy and Promote Growth? - https://carnegieendowment.org/files/Burman_Data_Privacy.pdf

This research by Anirudh Burman through an empherical study on the topic this paper argues that the bill does not correctly address privacy-related harms in the data economy in India. Rather than preserving information with an eye towards the harm that is results from its violation, the law seeks to protect the individual's information privacy by establishing a preventive framework that governs how corporates gather and utilize the information. The author also emphasize that given its cross-

sectoral mandate, the Data Protection Act may struggle to build internal capacity, leading to either under regulation or overregulation.

5. Privacy and Data Protection in an International Perspective-
   https://www.scandinavianlaw.se/pdf/56-8.pdf

The Author Lee A.Bygrave in this article provides a cross-jurisdictional review of the development of regulatory instruments to protect privacy and related interests with regard to the processing of personal data. The focus of the research is to present and compare briefly various national, regional and cultural conceptualisations of the ideals and rationale of privacy and data protection and at summing up basic regulatory patterns in the global data protection scene, the focus being the 'Big Picture'. He observes that though far-reaching laws are not widely established, however readiness to establish at least rudimentary regulatory equivalents is increasingly global.

1.5. **SCOPE OF THE RESEARCH:**

The scope of securing privacy in the era of computer vision in India can include, but is not limited to, Analyzing existing privacy laws and regulations in India and assessing their adequacy in addressing the challenges posed by computer vision technology. Recommending amendments or new regulations to protect individual privacy in the context of computer vision. Exploring techniques and strategies to protect personal data collected by computer vision systems. Investigating the ethical use of computer vision in India, paying particular attention to issues related to bias, fairness, and discrimination.

1.6.**OBJECTIVE OF THE RESEARCH:**

The primary objective of securing privacy in the era of computer vision in India is to strike a balance between reaping the benefits of computer vision technology and safeguarding individuals' privacy rights. The specific objectives can include:

1. Assessing the privacy implications of computer vision technology in Indian society, taking into account the privacy expectations and concerns of various communities.
2. Identifying gaps and weaknesses in existing legal and policy frameworks in India related to data privacy and recommending measures to address them effectively in the context of computer vision.

3. Working towards ensuring that the deployment and use of computer vision systems in India adhere to the principles of fairness, transparency, accountability, and respect for individual privacy.

1.7. RESEARCH QUESTION:

1. Are current privacy and data protection laws in India sufficient to address the unique challenges posed by computer vision, is there a requirement for revision and enhancement of the law?

2. What are the ethical issues and how can ethical guidelines and policies be developed and implemented to strike a balance between the benefits of computer vision and the protection standards in the era of computer vision?

1.8 RESEARCH METHODOLOGY:

In this research paper Empirical, Hermeneutic and Evaluative research has been followed throughout the paper. This research is based on both Primary and Secondary Data. Primary being the statutes, cases and books referred, while the secondary data being the articles, blogs, journals, website used for reference in the formation of the paper. These referred to understand the Background of the paper and in the formation of the Research question.

2. ARE CURRENT PRIVACY AND DATA PROTECTION LAWS IN INDIA SUFFICIENT TO ADDRESS THE UNIQUE CHALLENGES POSED BY COMPUTER VISION.

Computer vision is a specific form of Artificial Intelligence which uses the image recognition model to identify, process, store and give an output on the data. Therefore to regulate this, a regulating provision on Artificial intelligence related to Data Protection and Privacy can address the unique issues that may arise in the field of computer vision. In India, currently there are no specific provision that deals with Artificial Intelligence. Artificial Intelligence is regulated in India by the Ministry of Electronics and Information Technology (MeiTY). Any Development, execution, and administration of AI rules and regulations in India fall under its purview. There are certain provisions from various different acts and judicial pronouncements from which the protection of criminal or wrongful activity

using AI can be made liable, they are:

<u>Information technology act, 2000:</u>

The Information Technology Act, 2000 (IT Act) serves as the fundamental legislation governing electronic transaction and digital governance. Indian government enacted this legislation based on UNCITRAL's guidelines-UNCITRAL Model Law on Electronic Commerce (E-commerce) in 1996, which was later updated and approved by the Ministry of Electronics and Information Technology, becoming the Information Technology Act of 2000. Even though the Act doesn't specifically address AI, activities involving AI are covered by certain provisions of its sections.

- Compensation may be granted under Section 43A of the IT Act in the event that careless handling of sensitive personal data results in a data privacy violation. This clause is especially pertinent when it comes to AI systems that handle user data.
- IT Act,2000 punishes breach of privacy, section 66E, 72, 72A

<u>Indian copyright act, 1957:</u>

Original literary, artistic, musical, and dramatic works are protected under the Indian Copyright Act, 1957, which grants creators exclusive rights and forbids unapproved use or duplication. AI-generated material is becoming more and more prevalent, which has sparked debates over copyright ownership and infringement liability. Under the case of Gramophone Company of India Ltd. v. Super Cassettes Industries Ltd.[1], the Delhi High Court ruled in the 2011, that music generated by artificial intelligence software is not creatively created by humans and is therefore not protected by copyright. The copyrightability of AI-generated content in India is made clear by this case.

INITIATION OF DATA PROTECTION:

However, the turning point for the protection of personal data in India was the Supreme Court of India's Puttaswamy decision in 2017. This Supreme Court case of *Justice K.S. Puttaswamy (Retd) v. Union of India (2017)* [2]declared that the "right to privacy" is a fundamental right, paving the way for the drafting of a Personal Data Protection Bill and the enactment of a comprehensive privacy law in India. As stated by the court, privacy is a basic right or freedom protected by Article 21, which states that "No person shall be deprived

---

[1] NO.2382/2005 IN C.S. (OS) NO.399/2005
[2] W.P.(C) NO.000372/2017

of his life or personal liberty except according to procedure established by law."

Later, in the aim of enacting a data protection law, the Indian Planning Commission developed the National Strategy on Artificial Intelligence (NSAI) in 2018 and proposed forming a group with representatives from the Department of Industrial Policy and Promotion and the Ministry of Corporate Affairs to review the regulations.

A Joint Parliamentary committee recommended the Personal Data Protection Bill, 2019, which is based on a draught data protection statute. The Ministry of Electronics and Information Technology (MeiTY) made the proposal. Since personal data is gathered, transferred, and processed, it is also known as the Privacy Bill. The bill was pending before the lower house of parliament. On Wednesday, August 3, 2022, the Personal Data Protection Bill was withdrawn by the Central Government. Similarly, in August 2022, the government withdrew the Personal Data Protection Bill 2021. The Digital Personal Data Protection Bill 2022, which replaces the 2011 rules (IT rules, 2011, regarding reasonable security practices for the management of sensitive personal data or information), was introduced by the Ministry of Electronics and Information Technology on November 18, 2022.

DIGITAL PERSONAL DATA PROTECTION BILL, 2023

The 2019 bill provided for a preventive framework. This Bill allows for the processing of digital personal data in a way that respects people's rights to privacy protection as well as the necessity of processing such data for legitimate reasons and for purposes related to or incidental to those goals. Some of the key features of the Bill are:

1. The Bill offers the following protections for digital personal data:
    a) Data Fiduciaries' obligations for data processing;
    b) Data Principals' rights and duties; and
    c) Penalties for violations of rights, duties, and obligations.

2. The following seven concepts form the foundation of the bill:
    a) Consentent, lawful, and transparent use of personal data;
    b) purpose limitation;
    c) data minimization;
    d) data accuracy;

e) storage limitation;

f) reasonable security safeguards; and

g) accountability through the adjudication of data breaches and Bill provisions violations and the imposition of penalties for the breaches are the key points of accountability.

3. The Bill provides for following rights to the individuals:

a) The right to access information about personal data processed;

b) The right to correction and erasure of data;

c) The right to grievance redressal; and

d) The right to nominate a person to exercise rights in case of death or incapacity.

4. The Bill lays out the data fiduciary's responsibilities as follows:

a) to have security measures in place to prevent breaches of personal data;

b) to notify the affected Data Principal and the Data Protection Board of breaches of personal data;

c) to erase personal data when it is no longer needed for the intended purpose;

d) to erase personal data upon consent withdrawal;

e) to have a grievance redressal system in place and an officer to answer questions from Data Principals; and

f) to fulfil certain additional obligations in relation to Data Fiduciaries notified as Significant Data Fiduciaries, such as appointing a data auditor and carrying out regular Data Protection Impact Assessments to ensure higher degree of data protection.

5. The exemptions provided in the Bill are as follows:

a) For notified agencies, in the interest of security, sovereignty, public order, etc.;

b) For research, archiving or statistical purposes;

c) For start-ups or other notified categories of Data Fiduciaries;

d) To enforce legal rights and claims;

e) To perform judicial or regulatory functions;

f) To prevent, detect, investigate or prosecute offences;

g) To process in India personal data of non-residents under foreign contract;

h) For approved merger, demerger etc.; and

i) To locate defaulters and their financial assets etc3

LACUNAE OF THE BILL:

Deemed consent-

The Indian data protection regime introduces the concept of 'deemed' consent in Section 8, which allows a data principal's consent for processing their personal data in certain situations. This includes fulfilling lawful functions, public interest, and healthcare functions. Although initially problematic, this concept is similar to the principle of legitimate interests in the General Data Protection Regulation (GDPR), which applies when a company uses personal information in a way the data subject would expect. A re-writing of this provision is necessary to clarify the use of 'deemed' consent, which is a globally accepted practice.

Protection only on Personal data-

The bill mandated "sensitive" and "critical" personal data to have higher levels of security and classified personal data into various categories. Additionally, some companies were to be classified as "significant data fiduciaries," and they were to be subject to extra requirements such as data impact assessments, data audits, and registration in India. This completely exclude non personal data which may be acquired without consent of the individual by the researchers, product developers and other stakeholders.

Exemption under the Bill:

The Personal Data Protection Bill, 2019 and the DPDP Bill, 2022 provide exemptions for the government to process personal data in the interests of sovereignty, integrity, security, friendly relations with foreign states, public order, or preventing incitement to crimes. However, these exemptions lack concrete definitions, raising concerns about mass surveillance of citizens' personal data. This provision must be emphasized the importance of legality, necessity, and proportionality in exemptions.

---

3 Digital personal data protection bill, 2023. https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1947264

Section 17 of the Bill introduces an Allowist approach to data localisation, allowing data fiduciaries to share data with nations prescribed by the Union Government. However, this approach lacks clear selection criteria and guidelines for minimal data protection regimes, which is a serious issue as it gives too much discretion to the Union Government.

Since the computer vision technology of the Artificial Intelligence uses sizable enough data and deep learning to predict the possible outcome, the requirement of data is a crucial, while aiming the protection of individual's privacy. Due to the lacunae in the provisions of the Data protection Bill there may be possible chance of violation of right to privacy and breach of data protection, hence addressing these issues become a need of the hour.

3. WHAT ARE THE ETHICAL ISSUES AND HOW CAN ETHICAL GUIDELINES AND POLICIES BE DEVELOPED AND IMPLEMENTED TO STRIKE A BALANCE BETWEEN THE BENEFITS OF COMPUTER VISION AND THE PROTECTION STANDARDS IN THE ERA OF COMPUTER VISION?

Ethical Issue are concerned with how we perceive and utilise a particular information to decide our action in the real world, which may either be morally right or wrong. Machines can now see and understand visual data like never before thanks to major advancements in computer vision technology in recent years. Computer vision has applications in a wide range of industries, from face recognition systems, manufacturing, security surveillance, augmented reality, driverless cars, etc. But these developments have also given rise to ethical questions about the potential applications of computer vision technologies especially in the field of Facial Recognition and Security surveillance.

BIAS, INEQUALITY AND DISCRIMINATION:

Widespread usage of computer vision technologies may have profound effects on society. Because it disproportionately affects some populations, it may worsen already-existing inequities, such as socioeconomic inequality. For instance, The study, published in 2018, had trained algorithms to

distinguish faces of Uyghur people, a predominantly Muslim minority ethnic group in China, from those of Korean and Tibetan ethnicity Scientists should not acknowledge the morally dubious foundations of much of the academic work in the field especially which are biased and discriminatory, despite denouncing controversial uses of technology.[4]

INFORMED CONSENT:

Personal data is collected and analysed in computer vision applications frequently. People might not always understand, though, how much of their data is being collected and used. To enable people to make educated decisions about the use of their personal information, obtaining informed consent is becoming a crucial component of the ethical computer vision implementation process. Especially for facial-recognition algorithms to work well, they must be trained and tested on large data sets of images, ideally captured many times under different lighting conditions and at different angles. But most of the scientists now collect facial images without asking permission.

For instance, in 2016, researchers at Duke University in Durham, North Carolina, released more than 2 million video frames (85 minutes) of footage of students walking on the university campus.[5]

SECURITY AND SURVEILLANCE CONCERNS:

Though advances in security and surveillance are provided by computer vision technology, misuse can have dangerous effects. Significant ethical issues include the possibility of mass surveillance, unauthorised access to sensitive information, and cyber security vulnerabilities. To allay these worries, it is imperative to find a middle ground between personal privacy and public safety. For instance, in 2015, scientists at Stanford University in California published a set of 12,000 images from a webcam in a San Francisco café that had been live-streamed online[6].

ADDRESSING ETHICAL CONCERNS:

Owing to the aforementioned moral dilemmas raised by computer vision technology, it is essential to create and put into effect moral norms and guidelines in the age of computer vision in order to balance

---

[4] https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1947264
[5] https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1947264
[6] https://ebin.pub/vol-587-19-november-2020-nature.html

its advantages and protection requirements. Here are some actions to think about:

1. Gathering diverse perspectives by establish a multidisciplinary team comprising experts in computer vision, ethics, law, and relevant stakeholders, including representatives from various communities that may be impacted by computer vision. On establishment of such body, decisions regarding the policies which may protect the privacy and at the same time reap the fruit of computer vision technology can be arrived.

2. Define core principles and developing clear guidelines by collaboratively identifying and articulating core ethical principles that should guide the development and use of computer vision technology and evaluate potential risks associated with computer vision technology, such as biases in algorithmic decision-making, invasion of privacy, or unintended consequences. Assess the potential impact on individuals, communities, and society as a whole. Based on the core principles and risk assessments, create concrete guidelines and best practices for the development, deployment, and use of computer vision technologies by including recommendations for fairness, transparency, informed consent, data protection, and accountability mechanisms.

3. Establish legal and regulatory frameworks through ensuring that computer vision technologies comply with existing laws and regulations, such as data protection and privacy laws. Identify any gaps and work towards addressing them through additional regulations if necessary.

4. Encourage education and awareness though Promotion of awareness and provide educational resources to help people understand the capabilities, limitations, and potential impacts of computer vision technology. This empowers individuals to actively engage and make informed decisions regarding privacy and their rights.

5. Regularly review and update Computer vision technologies which evolves rapidly. Therefore, it is essential to establish mechanisms for regular reviews and updates of ethical guidelines and policies. This ensures they remain relevant, effective, and aligned with emerging societal and technological developments.

6. Monitor and enforce compliance and establishing mechanisms for monitoring compliance with ethical guidelines and policies. Encourage self-assessment, third-party audits, and independent evaluations of computer vision systems to ensure adherence to the established standards. Implement appropriate consequences for non-compliance to promote accountability.

Even though the prevalence of such ethical issues makes us to think twice about the need of Computer Vision. But the key to achieving the goal is to maintain a balance between the advantages of computer vision technology and the moral obligations and safety measures required to protect people and the community at large.

4. CONCLUSION:

Therefore, a system that uses artificial intelligence (AI) to enable computers to extract useful information from visual inputs is known as computer vision. *The insights gained from computer vision are then used to take automated actions. Though there are many benefits through this technology there are still issues involving computer vision. Hence its crucial to implement a robust security system, by addressing the lack and enforcing strict polices to avoid ethical issues. As Computer vision becomes more prevalent in various sectors, importance of educating public about the implications it has on their privacy and establishing a transparent, trusted and accountable governance is significant. That being the case, we urge the stakeholders like government, policy makers, researchers and technological developers, business & organisation to proactively engage by going hand in hand to develop a robust regulation policy and to revise the regulations as per the dynamic needs.*

REFERRENCES:

STATUTES:
- The Constitution of India, 1949.
- Information Technology Act, 2000
- Indian Copyright Act, 1957.
- Digital Personal Data Protection Bill, 2023.

BOOKS:
- Vakul Sharma's Information Technology Law and Practice (128-152) Lexis Nexis (7th edition 2022)

CASE LAWS:

- Justice K.S. Puttaswamy (Retd) v. Union of India (2017), W.P.(C) NO.000372/2017

- Gramophone Company of India Ltd. v. Super Cassettes Industries Ltd, I.A NO.2382/2005 IN C.S. (OS) NO.399/2005

RESEARCH ARTICLES:

- https://link.springer.com/chapter/10.1007/978-3-031-19149-7_5

- https://link.springer.com/article/10.1007/s43681-023-00272-x

- https://carnegieendowment.org/files/Burman_Data_Privacy.pdf

- https://www.scandinavianlaw.se/pdf/56-8.pdf

- https://go.gale.com/ps/i.do?id=GALE%7CA650829229&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=00280836&p=AONE&sw=w&userGroupName=tel_oweb&isGeoAuthType=true&aty=geo

WEBSITES:

- https://www.augmentedstartups.com/blog/exploring-the-ethical-implications-of-computer-vision-technology-in-2023

- https://blog.ipleaders.in/data-protection-laws-in-india-2/#Justice_KS_Puttaswamy_Retd_v_Union_of_India_2017

- https://clt.nliu.ac.in/?p=845

- https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1947264

- https://www.simplilearn.com/computer-vision-article

- https://www.allerin.com/blog/the-evolution-of-computer-vision-from-its-origins-to-modern-applications

- https://inbaviewpoint.org/laws-related-to-artificial-intelligence-in-india/

- https://www.legalserviceindia.com/legal/article-13111-laws-governing-ai-in-india-everything-you-should know.html#:~:text=Legal%20provisions%20governing%20AI%20in%20India&text=However%20recently%2C%20IT%20Minister%20Ashwini,with%20Ai%20growth%20in%20India.

- https://ebin.pub/vol-587-19-november-2020-nature.html