EXPLORING THE IMPACT OF EMERGING TECHNOLOGIES ON CRIMINAL PROCEDURE, SUCH AS FACIAL RECOGNITION, BIOMETRIC DATA, AND SURVEILLANCE TECHNOLOGIES

Kumar Dhruva, LLM, Amity Institute of Advanced Legal Studies, Amity University, Noida

ABSTRACT

Emerging technology have significantly impacted India's criminal law, affecting different facets of the justice system, investigations, and law enforcement. To claim that technology exclusively has drawbacks would be inaccurate. If we look at the product images, we can see that there are many more advantages or benefits that technology can offer to all people. If technology is used properly, it can be demonstrated to be the greatest advantageous invention created to date. The sole need is that it be used, and that using such technology must not be done with malice. The time has come for us to begin utilizing such technologies for the benefitof our justice system. Numerous improvements are necessary for the Indian criminal justice system as a whole because it is in such bad shape. The requirement for a legal background to use technology in the criminal justice system to its full potential will also be discussed in this essay.

In order to make the best use of technology moving forward, we will address the future of newtechnology, its effects on the criminal justice system, and the legal context in this research paper. We'll also observe how the nations are improving their criminal justice systems by utilizing modern technology. India is also planning to use such technologies to improve the current criminal justice system.

Keywords: Criminal Justice system, Future advantages, Emerging technologies, Law enforcement

STATEMENT OF PROBLEM

The Modern world is altogether a different place to live in, everything has gradually moved towards modernization. Modernization has also creeped into law and justice. Technological advancement has made justice more accessible. The major concern that we will discuss in this paper revolves around merits and demerits of technology in legal field.

RESEARCH QUESTION

- Has modern technology impacted the legal justice system? If yes then in what sense,positive or negative?
- What are the major grey areas wherein Criminal laws in India need to evolve in order to be more justifiable with the help of modern technologies?

RESEARCH OBJECTIVES

- To understand how far is it feasible for technological aspects to step into legalaspects?
- What are the challenges that the legal system will have to face if technologicaladvancements are made?

HYPOTHESIS

The research paper will try to deal with hypothesis that Indian Legal system must go through achange and technological enhancement to make justice more accessible.

INTRODUCTION

Recent years have seen a great deal of debate and discussion over the effects of new technology on criminal law and the criminal justice system. The criminal justice system is facing new difficulties as a result of the lightning-fast speed of technology advancement, particularly in the areas of privacy, data protection, and law enforcement authority.

Many claim that the acquisition and use of personal data by law enforcement authorities breaches people's right to privacy, which has become a contentious topic in recent years. Many

jurisdictions have established data privacy regulations that restrict the gathering and use of personal data by law enforcement organizations in response to these worries. However, there is still disagreement regarding how well these rules safeguard people's privacy in the face of quickly developing technologies.

Emerging technology have sparked questions about the capabilities and constraints of law enforcement organizations in addition to privacy issues. For instance, the use of facial recognition technology by law enforcement organizations has come under fire for the possibility that it would be racially and discriminatorily biased. Concerns regarding the possibility of misuse and the violation of individual rights have been expressed in relation to other developing technology, such as drones and automated surveillance systems.

Overall, the effect of new technology on the criminal justice system and the law is a complicated and continuous topic that necessitates constant discussion and debate. In order toprotect people's civil liberties and privacy as technology develops, it will be critical to find a balance between the advantages and hazards new technologies provide.

Numerous forensic science developments that have emerged recently are altering how criminalcases are investigated and prosecuted.

HOW EMERGING TECHNOLOGIES AFFECT CRIMINAL LAW AND THE CRIMINAL JUSTICE SYSTEM

Nature's law states that nothing can be hidden. It is inevitable that there will be a drawback if we take advantage of something. The same is true when using emerging technologies. In this study, we'll talk about the different effects of using these tools to improve and develop the criminal justice system, but we'll mostly ignore how they'll affect people. The effects that thesetechnologies have on the criminal justice system cannot be discounted or disregarded. Additionally, it's crucial to address every single component of it. As a result, this study will assist us in comprehending the effects of the use of such technology as well as any potential solutions.

There is much to be done to lessen the influence of new technology on the criminal justice system, and the authorities in charge of its implementation must play a part in it. To decrease the influence of the technology that we are supposed to employ for our system, proper

technique and care are necessary. Only the government and its agencies will play a key role inreducing the impacts because they are in charge of how it is applied in society.

It's not accurate to say that the effects of technology cannot be lessened or at all. The answer isyes, but the essential requirement is ongoing and continuous consideration of the search for such solutions that will significantly contribute to the advancement of such technologies.[1]

It is true that there are now a number of risks associated with the integration of developing technology into our legal system.

ADVANCES IN CRIMINAL LAW AND THE JUSTICE SYSTEMTECHNOLOGIES

Any field has always benefited from technology. It is crucial to life from a person's conception till their passing. Technology can be used in many different ways, but it can also be abused. What does the word "emerging technologies" mean? Does this imply that the available technology is finite and has a finite purpose? The topic of emerging technology is one that is currently in prototype form but has not yet been fully and effectively utilized, which is the answer to this question.[2]

The term "emerging technologies" Particularly in the legal field, there is no clear definition of emerging technology. In plain terms, it can be described as a recent development in technology.Although their applications are still being researched, they are not the only ones. When an existing technology is altering its dimensions, it can also be referred to as an emergent technology. These technologies are employed in every industry, including business, education,and science.

Every industry is using rising technology in their own fields. AI is everywhere, and it can be leveraged to make some historic changes that future generations will never forget. It may be argued that AI can currently assist in the detection of small to serious disorders in the human body if we look at the healthcare sector. The employment of emerging technologies is also beneficial to the education sector, if we take a closer look. The future of education will also

[1] Lakshminath, A. "CRIMINAL JUSTICE IN INDIA: PRIMITIVISM TO POST-MODERNISM." 48, no. 1 Journal of the Indian Law Institute 26 (2006)
[2] Boxerman, Sanford J., and Michelle Feit Schwerin. "CRIMINAL JUSTICE: VIRTUAL CURRENCY: REGULATORY AND CRIMINAL LAW IMPLICATIONS." 34(3) GPSolo 72 (2017).

shift as a result of the application of AI technology.

Apart from the ruling in K.S. Puttaswamy v. Union of India[3], there is nothing more to be found in India when it comes to privacy, both legally and practically. Bills pertaining to data protection have been pending for years. After pulling the first draft back a few months ago, theadministration introduced a new one. Data privacy and other challenges relating to the technologies we are utilizing to improve the future still require a lot of work.

EMERGING TECHNOLOGY EXAMPLES

For the purposes of this study, it would be difficult to include all of the instances of emerging technologies due to their rapid expansion, but there are undoubtedly some that are more well-liked than others. These new technologies include;

1. Facial Recognition: The biometric technique that is most frequently used to recognize a person's face and identity is facial recognition. However, there is a great deal of privacy and bias against the use of facial technology[4]. This technology can be used to detect humans for the purpose of enforcement and occasionally even the missing individual. It can also be argued that facial recognition technology is prejudiced against nature and does not offer 100% accuracy.

2. Artificial intelligence is another intelligent species that can even build machines to carry outtasks that humans are incapable of carrying out. Data analysis, decision-making, natural language processing, and other tasks are among the many things the AI can do. Additionally, it's critical to recognize that the employment of AI in various governmental and non-governmental organizations raises a number of ethical and privacy concerns.

3. Virtual reality is a technique that uses computer generated imagery to simulate a real-world experience. This technology can be utilized for training purposes, and it is particularly useful in the criminal justice system to prepare officers for situations that are impossible to show. Thecriminal scenes can also be recreated using virtual reality for the purpose of investigation and gathering evidence. A significant and original advancement in technology as well as the

[3] (2017) 10 SCC 1
[4] Littler, Alan. "Internet-Based Trade and the Court of Justice: Different Sector, Different Attitude." 2, no. 1 European Journal of Risk Regulation 78 (2011).

criminal justice system is virtual reality.

4. Speech recognition is another piece of technology that can be used to recognize people basedon their speech or sounds. This technology is employed in the criminal justice system to authenticate and identify the people, either through our suspects or missing.

5. Automation: Another technology that is frequently employed in the criminal justice system and for other purposes is automation. Such technology has the advantage of making it possibleto organize tasks that are a little challenging for a human to complete.

6. Forensics: Forensics is a technology that has been in use for a very long time; in fact, it can be argued that it is primarily a full science. However, some breakthroughs and developments have been made in relation to forensics and the interaction of technology. The criminal judicial system is using recently invented technology[5].

7. Call data record: It's crucial to remember that a lot of call data records are also recorded andpreserved. Various law enforcement agencies use a variety of local and remote software to maintain the store. A data record is highly vital in any criminal investigation and aids in keepingtrack of any suspects, so keep it up.

TECHNOLOGY FOR FACIAL RECOGNITION

Law enforcement organizations all across the world have embraced facial recognition technology as a tool for locating and identifying people. However, there are serious privacy and civil rights issues created by its use. This study will look at how facial recognition technology is used by law enforcement, its possible advantages and disadvantages, and how itaffects civil liberties.

The capability of facial recognition technology to swiftly and precisely identify people is one of its key advantages. Since face recognition may be used to identify suspects and match themto surveillance footage, it can be especially helpful in criminal investigations. Facial recognition technology can also be used to track people who may be wanted by the law, such

[5] Rao, K. Sreedhar. "CRIMINAL JUSTICE SYSTEM — REQUIRED REFORMS." 43, no. 2 Journal of the Indian Law Institute 155 (2001)

as runaways or known criminals[6].

Law enforcement's use of facial recognition technology, nevertheless, also brings up a numberof issues. The possibility for technology abuse and misuse is one of the key worries.

For instance, using facial recognition technology to specifically target immigrants or people ofcolor for monitoring and investigation. Furthermore, the tracking of people who have not committed any crimes using facial recognition raises issues with privacy and civil liberties.

OVERVIEW OF FRT'S APPLICATION IN LAW ENFORCEMENT

Law enforcement organizations all around the world are increasingly using facial recognition technology (FRT) to identify suspects and find criminals. Law enforcement can employ this technology in many different ways, such as:

***Surveillance*:**

FRT can be used to analyze CCTV material to find suspects either immediately or afterwards.

***Matching mugshots*:**

FRT can be used to identify suspects who have previously been arrested by matching a person's facial features against a database of mugshots.

Persons missing:

FRT can be used to locate a missing person by comparing their face traits to those of known people in a database.

FRT can swiftly and effectively identify people, even if they are attempting to hide their identity, which is one of its key advantages for law enforcement. When responding to an active shooter or terrorist attack, for example, this can be especially helpful as time is of the importance.

However, privacy advocates have also challenged the use of FRT by law enforcement. Concerns about the technology's accuracy, potential for abuse, and effect on civil liberties

[6] https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt

are just a few. Furthermore, there are worries that particular communities, such as marginalized groups and people of color, may be adversely affected by the technology[7].

The employment of FRT by law enforcement is, in general, a difficult topic that necessitates comprehensive analysis of the advantages and disadvantages of the technology.

FRT'S ADVANTAGES IN LAW ENFORCEMENT

Law enforcement could be revolutionized by facial recognition technology (FRT), which offersa valuable tool for identifying criminals and solving crimes. Being able to identify people fastand precisely is one of FRT's primary advantages in law enforcement. This can be especially helpful in circumstances where traditional identifying techniques like fingerprints or DNA analysis are impractical or impractical.

The ability of FRT to increase public safety is another benefit to law enforcement. FRT can aidin crime prevention and stop dangerous people from committing more crimes by giving law enforcement the capacity to swiftly identify suspects. FRT can also assist law enforcement in finding missing people more quickly and effectively, which can result in quicker resolutions and better outcomes for the missing person and their loved ones.

By automating some processes, FRT can also assist in lightening the workload of law enforcement employees. This may increase the effectiveness of law enforcement organizationsand free up more resources for use in other crucial areas. Additionally, by giving law enforcement more thorough information about suspects and prospective witnesses, FRT can aid in making criminal investigations more accurate.

Finally, by offering a more precise and effective means of identifying suspects, FRT can contribute to bettering community relations. This can aid in lowering the amount of erroneousdetentions and boosting public confidence in law enforcement. Additionally, FRT can aid in lowering the amount of erroneous convictions by giving law enforcement a more precise and effective way to identify suspects.

In conclusion, FRT has a number of benefits for law enforcement, including the ability to

[7] Facial Recognition Technology in India August 31, 2021 By Elonnai Hickok, Pallavi Bedi, Aman Nair and Amber Sinha Reviewed by Daragh Murray, Peter Fussey, Amy Stevens and Arindrajit Basu, The Centre for Internet and Society, India

precisely and rapidly identify people, increase public safety, lessen the strain of law enforcement employees, increase the precision of criminal investigations, and enhance community relations. However, it is crucial to keep in mind that the use of FRT also presents issues related to civil liberties and privacy. As a result, it is crucial to make sure that the use of FRT is done in a way that respects and protects individual rights[8].

INVESTIGATION AND CRIME PREVENTION

The use of facial recognition technology (FRT), a potent tool, in criminal investigation is growing. It is a computer-based system that can recognize faces in digital photos or videos andmatch them to faces in a database. This technique is used to find missing people, identify victims of large-scale disasters, and identify suspects in criminal investigations[9].

FRT can also be used to keep an eye on public areas and follow people's activities in real time, which can help stop crime before it happens. It has been extensively employed in the investigation of crimes like theft, robbery, and murder. FRT is now being used by law enforcement agencies all around the world to aid with their investigations. But this technologyis not without controversy; the primary ones being privacy issues and possible algorithmic biases.

PROBLEMS AND RESTRICTIONS WITH FRT

Facial recognition technology (FRT) is a potent instrument that can help with criminal investigations and crime-solving. However, using this technology comes with a number of difficulties and restrictions.

The possibility for bias in the facial recognition algorithms is one of the major problems. These algorithms frequently perform less accurately for people with darker skin tones or non-binary gender identities, according to studies. This may result in erroneous identifications and arrests. Additionally, elements like lighting, angle, and facial expressions can have an impact on facial recognition accuracy, making it challenging to find a precise match.

The lack of technological standards is another difficulty. Comparing findings across different

[8] https://www.computer.org/csdl/special-issue/pami/2022/03/index
[9] JUSTICE, BENJAMIN, and TRACEY L. MEARES. "How the Criminal Justice System Educates Citizens." 651 The Annals of the American Academy of Political and Social Science 159 (2014).

agencies can be challenging because different systems utilize various algorithms and have varying degrees of accuracy. Confusion and mistakes in investigations may result from this aswell.

Another significant drawback of facial recognition technology is privacy issues. Biometric datacollection, storage, and exchange creates issues with privacy and the possibility of power abuse. The public is also concerned that facial recognition data could be breached or stolen, which could result in identity theft or other types of fraud.

Last but not least, there are ethical issues surrounding the usage of facial recognition technology. Concerns concerning civil liberties, human rights, and the right to privacy are brought up by the usage of this technology. It's critical to balance the advantages of facial recognition technology against any potential concerns because its effects on society are still being investigated.[10]

Overall, even if facial recognition technology has the potential to be a useful tool in criminal investigations and crime-solving, it is vital to take into account the difficulties and restrictionsrelated to its use.

FRT'S EFFECT ON CIVIL LIBERTIES

The potential impact of facial recognition technology (FRT) on civil liberties is significant. One way to use it is to increase security and make it simpler to recognize and monitor offenders. For instance, FRT can be used to locate suspects in security footage, aiding in the investigation of crimes and the prosecution of offenders.

Concerns concerning the possibility of using FRT to violate civil liberties, however, are also very serious. One significant issue is that FRT might be used to secretly observe people without their knowledge or agreement, enabling governments and commercial entities to keep tabs onpeople's whereabouts and activities. Loss of privacy as well as a restriction of free expression and other basic liberties could result from this.

FRT could be used to discriminate against particular groups of individuals, which is another issue. For instance, if the technology is not calibrated properly, it may be more likely to

[10] Duraiswami, Dhiraj R. "Privacy and Data Protection in India." 6, no. 1 Journal of Law & Cyber Warfare 166 (2017).

incorrectly detect people with darker skin tones or specific facial traits. Racial profiling and other types of discrimination might result from this.

FRT might also be utilized to establish a "surveillance state" where the government can keep tabs on citizens' actions and stifle dissent. In the private sector, it can be used to collect client information for targeted advertising or other uses[11].

Overall, FRT has the ability to harm civil liberties significantly while simultaneously having the capacity to increase security and make it simpler to identify offenders. Governments and commercial organizations must carefully weigh the potential effects of employing this technology and implement strict rules and oversight to safeguard human freedoms.

REGULATORY AND LEGAL FRAMEWORK

Facial recognition technology's (FRT) legal and regulatory environment is still developing and differs by nation or region. Although some states and towns have passed their own restrictions,there is currently no federal law in the United States that governs the usage of FRT. For instance, FRT use by law enforcement has been outlawed in San Francisco and Oakland, California, while it has been put on hold in Boston and Portland, Oregon. According to legislation in some areas, including Texas, Illinois, and Washington, businesses must acquire consent before collecting any biometric data, including face recognition data.

Regulations for the use of FRT and other types of personal data are set forth in Europe by the General Data Protection Regulation (GDPR). Furthermore, the European Union is now draftingfresh rules tailored especially for FRT. This includes the proposed rule on AI, which will establish stringent guidelines for the application of FRT, including openness, human monitoring, and data minimization.

China and India in Asia have put national rules and regulations for the usage of FRT into effect. While India has been employing FRT for various government programs like Aadhaar and Real-Time Face Recognition System, China has established a national standard for FRT and has been exploiting the technology for surveillance and security purposes.

It is significant to note that laws and regulations pertaining to FRT are continually changing,

[11] Duraiswami, Dhiraj R. "Privacy and Data Protection in India." 6, no. 1 Journal of Law & Cyber Warfare 166 (2017).

therefore it is advised to keep up with the latest information on this subject.

FUTURE PROSPECTS AND SUGGESTIONS

Facial recognition technology's (FRT) future is uncertain, with both potential advantages and drawbacks. FRT has the potential to increase convenience and security in a variety of applications, from unlocking smartphones to identifying criminals, on the one hand. The healthcare sector and other sectors could benefit as well.

On the other hand, privacy issues and the potential for technology misuse, particularly in the context of mass surveillance, are worries. Additionally, there are issues with the bias and accuracy of some FRT systems, especially when it comes to people from marginalized groups.

Given these worries, it is advised that the development and application of FRT be governed bya strong set of ethical norms, such as accountability, openness, and respect for civil rights and privacy. Additionally, it's crucial to make sure that the technology is rigorously and objectivelytested and assessed, and that the right safeguards are put in place to lessen any potential bad effects. Furthermore, it is necessary to enact laws and rules that guarantee monitoring and accountability for the use of FRT.

PRIVACY AND DATA PROTECTION-RELATED ISSUES

The introduction of technology was made to improve and enrich human lives. In order to improve the criminal justice system, governments all over the world began to embrace technology. However, there are always two sides to a story. On the one side, technology greatly improves people's life, but on the other, there are a lot of worries attached to it as well.

Many academics and campaigners are drawing attention to the issues that are related to the useof developing technologies in the field of criminal law.

(A) PRIVACY ISSUES WITH NEW TECHNOLOGY

The technology was established with the intention of promoting the advantages associated withthem, such as their effectiveness and the various other functions they may carry out. However, technology cannot function independently and needs a variety of resources, including data. Data without technology is akin to a person without blood. If they are not

connected, one cannotlive without the other, then the other is useless.

There is no law in India that expressly addresses the issue of privacy. Although the Information Technology Act of 2002 does exist, it is not well suited to address the issues with data privacy that exist today.

The Hon'ble Supreme Court ruled in Justice K.S. Puttaswamy (Retd) v. Union of India that Part III of Article 21 of the Constitution protects one's right to privacy[12].

This ruling has the result that the court has correctly acknowledged the right to privacy. This means that it is imperative to defend everyone's fundamental right to privacy.

We will observe a significant drawback of information technology, namely the misuse of stored data, if we begin to integrate their use in our criminal justice system. It was discovered that police officers in California were abusing the technologies they were given access to. Anywhere the same thing can occur.

The fact that using technology is not simple must be discussed in relation to the employment of new technologies for the criminal justice system. It needs a lot of resources and money.16 The fragility of technology is another issue or worry related to its use. If one person can access something while being at a remote location, why can't the other person do the same by making a few simple changes? It is undoubtedly conceivable, which is why it is stated that technology is both a blessing and a curse.

It would therefore be accurate to state that it is simple to highlight the susceptibility of new technology when it comes to its application in the criminal justice system and law enforcement.

Given the Supreme Court's ruling and Article 21 of the Constitution, it is accurate to say that we do have a right to privacy that can be disregarded and disregarded simply because using new technology is more effective than using conventional methods that may also be used in the criminal justice system.

(B) DATA PROTECTION ISSUES RAISED BY NEW TECHNOLOGIES

The usage of developing technologies is also accompanied with difficulties with data

[12] Writ Petition (Civil) No 494 of 2012; (2017) 10 SCC 1; AIR 2017 SC 4161

protection. Let's first discuss the definition of data protection, which is defined by the Storage Networking Industry Association SNIA as "the process of safeguarding important data from corruption, compromise, or loss; and providing the capability to restore data to a functional state should something happen to render the data inaccessible or unusable."

In layman's words, it can be described as safeguarding data from misuse of any form and keeping it so that no negative effects can befall it. It entails safeguarding, managing, maintaining safety, and mitigating any additional negative consequences on it. The three categories of "traditional data protection, data security, and data privacy" may be seen when we look at the different forms of data.

Utilizing new technology presents a number of difficulties, including

1. Wide access: Technology seeks to provide wide access, but this also opens the door formisuse. It makes sense since the further technology moves, the more likely it is to be misused. Most people and businesses do not give much thought to protecting their personal data, which can subsequently result in issues when they have to deal with theconsequences of its exploitation. This is the reason why those who anticipate engagingin these actions later on uncover gaps and gain access to a sizable, insecure network.

2. Threats to security come in many forms and have a significant part in the misuse of developing technologies. Let's start by examining the threat to cyber security. It impliesthat such criminals who wait for an opportunity to abuse such technology are exposed in the cyber world. They watch for the ideal moment to break into the system and hackthe available data. Later, they sell these data to others who can profit from its misuse.

   Today, hacked data is readily available on some websites, and those who wish to utilize it can purchase it there.

3. High record: Data is kept in memory, which also calls for high storage. We lack adequate legislation governing the storage of data that is stored for the purpose of law enforcement in the absence of any explicit regulations.

4. Safety measures: Data protection calls for safety measures, commonly referred to as

antivirus software or data protection devices. More safety is needed since there is moredata present. In a similar vein, when agencies intend to deploy cutting-edge technologies in the criminal justice and law enforcement systems, they also need to ensure their security. Given the current system, it is urgently necessary to plan the safetymeasures before implementing the use of emerging technologies in the criminal justicesystem. There is a big need for safety devices that need to be installed for the protectionof such big data that is stored on the server so that it cannot be misused further.

THE 2002 INFORMATION TECHNOLOGY ACT

The information technology act's primary goal and objective was to control electronic records,including signatures on documents and other items crucial to the technical world. Earlier, the legislature could not anticipate India's impending adoption of the technology or the domain- specific nature of concerns relating to developing technology. Although the Legislature did notintend for this act to address issues of data protection and privacy, it has evolved as a result ofjudicial decisions and revisions. Two of the most significant rulings using the IT Act are thosein the cases of Tehsin S. Poonawala and Shreya Singhal.[13]

However, there are several legal measures that deal with safeguarding against technology-related crime, including cybercrime.

DIA, OR THE DIGITAL INDIA ACT

In India, the digital and technological industries have been governed under the Information Technology Act since 2002. The current IT Act was created in an effort to curb the technology-related issues that were then rampant. The IT Act, however, cannot address the problems brought on by the development of technology because it is an outdated piece of legislation. Asa result, the Indian government intends to replace it with new legislation. To address the issues with technology in India, the government wants to create a more dynamic and comprehensivelaw. What distinguishing traits does DIA have?

With relation to digital intermediaries, their liabilities, and their obligations as a medium, the DIA is anticipated to alter the current safe harbor. The government believes that digital

[13] https://www.livelaw.in/pdf_upload/letter-petitionnuh-violence-and-its-aftermath--486980.pdf

platforms cannot avoid their responsibility for any action that occurs on their platforms, despitetheir demands for immunity. They have a duty to keep an eye on and control things on their own platform.

Another essential component of DIA is the growth of the open internet. This is based on the increase in players in the digital market. The government has also established a committee to study the necessary revisions to the current competition statute in light of the digital market. The DIA will also prioritize giving market participants a level playing field. Regarding digitalcompetition, the DIA and the ministry intend to significantly amend the current Competition Act, 2002[14].

The DIA places a major emphasis on giving online users safety and security. Because there have been more instances of online fraud, crimes, and traps in recent years, the government isseeking to make the internet a safer place. Children will receive special attention so they won'tfall prey to online traps. This will also fix who is responsible in the event of a mistake.

The DIA will also work to reduce the spread of incorrect information and fake news nationwide. In order to stop fake news, the government plans to create some strict compliancesthat intermediaries must follow.

The DIA will also control the spread of artificial intelligence across a variety of industries, including finance, healthcare, and education. This will address the technologies that are now in use, including blockchain, Web 3.0, and machine learning. New guidelines and restrictions for these technologies will be provided by the DIA. Because cybersecurity is not specifically included in the current IT statute, DIA will introduce legislation specifically addressing it. TheDigital India Act will continue to put user privacy and safety first.

The DIA will also work to safeguard users' rights related to technology use, such as "the right to be forgotten" and "the right against discrimination," among others. The DIA will also concentrate on privacy-invading gadgets like spy cameras, wearable technology, etc. In the name of the right to free speech and expression, it would monitor fake news on social media.

[14] https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf

POWERS OF LAW ENFORCEMENT

(A) LEGAL CONCERNS ABOUT THE AUTHORITY OF POLICE ENFORCEMENT

Although technology has been a useful tool in law enforcement and other areas of the legal profession, law does not necessarily oppose it. The law, on the other hand, is all about defending a person's and a person's rights. In that regard, using cutting-edge technology in thecriminal judicial system presents some difficulties and legal concerns.

The right to privacy is included as a fundamental right under the rights to life and personal liberty in Article 21 of the Indian Constitution. The right to privacy has also been upheld as a fundamental right by the Supreme Court of India on numerous occasions. As a result, the fundamental right to privacy is a recognized fundamental right in India, and the use of new technology in the criminal justice system infringes on that right for people who fall under the first Technology circle.

The usage of such technologies in the criminal justice system is not well suited for police officers and law enforcement agencies. Because of this lack of training, there have been numerous instances of authority abuse. Even the judges and other individuals charged with using such technology are unable to fully utilize them. The use of such technology to enhance the criminal justice system comes with a considerable danger as well.

As a result, there is a significant need for employees who will use this technology to receive appropriate training and specific experience. Along with legal concerns, using such developingtechnology raises ethical ones as well. Police are supposed to follow an ethical code, but in practice they often don't know what it is, leading them to commit immoral and unacceptable activities. Therefore, if the government intends to add more technology to the criminal justicesystem in the near future, proper training and understanding are needed.

Therefore, even if data vulnerability may not be a legal concern, making a technology vulnerable does have an impact on those people. If hackers discover a system vulnerability, it may be argued that everyone will have access to the data kept for legal reasons in sportsman. They can simply use such priceless information for their own gain. The use of such cutting- edge technologies in the administration of the criminal justice system is thus seriously threatened by the legitimacy of the data.

As a result, it can be claimed that utilizing developing technologies in the criminal justice system is crucial and that doing so raises a number of legal difficulties. Although there are things that organizations and the government may do to address these problems, they cannot be totally eliminated. Other things must be done with the people who are trusted to utilize thistechnology, in addition to fixing these problems[15].

(B) MAINTAINING A BALANCE BETWEEN DATA PROTECTION AND LAW ENFORCEMENT AUTHORITY

The use of technology is crucial in the modern world. Nowadays, leaving the house without using technology is all but impossible. One cannot entirely stop using technology. It's because using such technology to perform our tasks requires it of us as humans. Additionally, it is truethat technology has always been essential to human existence. The same is true for the law enforcement organizations. Such organizations also need this support. Because of this, it is impossible to maintain a balance between the criminal justice system and law enforcement by using developing technology. It's important to strike a balance between the use of technology and data privacy protection.

Things must be done in order to maintain the equilibrium, including:

1. Training properly: Those using technology need to receive training that is done properly. This includes representatives from other law enforcement organizations including the cyber cell police. Their education must be structured in such a way that professionals from these fields inform them of all the potential abuses of such cutting-edge technology.

2. High Security: To lessen the impact of developing technologies on the criminal justice system, high-security measures must be implemented. Additionally, it involves setting up servers that will safeguard the stored data.

The security of such data is crucial to preserving individual privacy and preventing the potentialfor misuse in the event that the wrong people come into possession of it. As a result, the storageof such vulnerable data that is kept by agencies requires proper and strong security.

[15] Rao, K. Sreedhar. "CRIMINAL JUSTICE SYSTEM — REQUIRED REFORMS." 43, no. 2 Journal of the Indian Law Institute 155 (2001).

CONCLUSION

It is evident from the study above that the criminal justice system regularly makes use of developing technologies by law enforcement agencies and other government departments. There are other nations with more sophisticated technology than India that also engage in thisbehavior. The technique has been utilized by numerous nations for a very long period. The criminal justice system and police department productivity in India are now being improved through the use of such technology by many states and Central government entities.

There is a significant need for India to develop rules and regulations in this area. India currently lacks any explicit legislation dealing with the adoption of such Technology. Additionally, India lacks the data protection act, which is crucial in the modern technology era. In the absence of laws, it is crucial that India and any law enforcement agencies that use this technology adhereto it. This is bad for the criminal justice system and will raise a number of issues, including privacy and prejudice. The goal and purpose behind developing a criminal justice system willbe somewhat disturbed by this, and the fate of individuals will be lost.

Law enforcement agencies are utilizing cutting-edge technology for the criminal justice system, including surveillance, biometric data collection, electronic monitoring, and other technologies. While there is no denying that such technology is very beneficial for the goals ofthe criminal justice system, it is crucial to recognize that there are a number of issues that mayarise. The privacy rights are one such major issue with regard to technology use in the criminaljustice system.

The government agency should be more honest and explicit about how the privacy is safeguarded when using this technology. This is also alarming since there is a risk that some of those bed components will misuse the technology when we Agencies employ it. The government needs to develop some effective strategies to address the technological problems.

The use of biometric and surveillance technology poses a serious threat to personal safety. Sometimes someone will utilize fingerprints or other digital prints of different people for a crime scene with the goal to commit fraud. Such situations call for prudence, and the government should guarantee that no one is authorized to access sensitive data.

Having strong legislation to address these issues is the only practical remedy for privacy issues.

It is crucial that government organizations are aware of and consider the potential impacts of implementing cutting-edge technology for the criminal justice system. In order to prevent further abuse of this technology, it is also the duty of the government to teach these officials.

It is also crucial that government organizations develop additional solutions to handle issues that could develop in the future. India is currently adopting this technology in its criminal justice system for the very first time, therefore the risk is currently relatively low. Such issues must be reduced as soon as possible in order to make future issues manageable. Technology has the ability to significantly alter society, therefore eliminating it without looking for a solution is impossible. Thus I would Like to Conclude by Stating that my Hypothesis stands proved.

BIBLIOGRAPHY

- Dudarev V. A., “COVID-19 Pandemic as a Catalyst for Digitalization of Russian Criminal Justice”, Russian Journal of Criminal Law, vol. 17, pp. 39-43. (in Russian)
- Kim D. V. (2021) “Modern trends in the development of forensic techniques and technologies in criminal proceedings”, A. I. Bayanov, (Krasnoyarsk, 2021)
- Mailis N.P. (2022) “The role of innovative technologies in the development of digital traceology”, Theory and Practice of Forensic Science, vol. 17, no. 2, pp. 18-22. (in Russian)
- Mishra B., Chatterjee S., & Mishra S. (2021) “Traditional judicial systems need ammunition for future”, Journal of Legal, Ethical and Regulatory Issues, vol. 24, no. 2,pp. 1-14.
- Mishra U. (2021) “Application of Cyber Forensics in Crime Investigation”, IJRAR-International Journal of Research and Analytical Reviews, vol 5, no. 3, pp. 317-322.
- Dr. O. Gambhir Singh. (2018) “Artificial Intelligence in Forensics & Criminal Investigation in Indian Perspective”, International Journal of Innovative Science and Research Technology, vol. 7, no. 7, pp. 142–144, https://doi.org/10.5281/zenodo.7008330