IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

BALANCING POLICE POWERS AND PRIVACY RIGHTS: A CRITIQUE OF THE CRIMINAL PROCEDURE IDENTIFICATION ACT 2022

Anushka Sharma
Student
Institute of Law, Nirma University

ABSTRACT

This article scrutinizes the interplay between police prerogatives and the right to privacy under the recently enacted Criminal Procedure Identification Act 2022. Drawing on the evolution of privacy rights in American and Indian jurisprudence, the study delves into key cases like Roe v. Wade, illuminating the development of individual autonomy in privacy matters. It further explores the emergence of the "right to be forgotten" doctrine in India, underscoring the expansion of privacy rights in the digital age.

The article introduces the innovative provisions of the Criminal Procedure Identification Act 2022, which harnesses technological advancements for investigative purposes, including biometric identification and electronic surveillance. Employing a critical lens, the Act's compatibility with the right to privacy is evaluated, elucidating potential implications for personal liberties and due process.

Analysing the Act's implications, the study highlights potential conflicts between effective law enforcement and safeguarding privacy. It underscores the need for a judicious balance between police powers and constitutional rights, in line with democratic principles. The article concludes by advocating for a harmonious coexistence between the Act's provisions and the right to privacy, emphasizing the importance of maintaining societal equilibrium while upholding individual freedoms.

Keywords: *Right to Privacy, Criminal Procedure Identification Act, Police Power, Law Enforcement, Right to be Forgotten, Constitutional Rights, Technological Advancements.*

INTRODUCTION

The recently passed *Criminal Procedure (Identification) Act* has sparked numerous demonstrations by proponents of human rights. In criminal cases, this statute takes the place of colonial identification and investigation. Additionally, it permits the storage of documents and data. The 87th Law Commission report evaluated the previous criminal identification act for the first time in 1980 and made several recommendations for revisions, which led to the first realization that this law needed to be amended. The judgement of the *State of UP v. Ram Babu Mishra*,[1] served as the backdrop for this legislative action.

This act allows the police to use various technologies to take accurate body measurements of convicts, accused, and other individuals. Governance must be current with the world at large in this high-tech era. Nowadays, artificial intelligence has outpaced itself and advanced quite quickly. Therefore, the ability of the executive to quickly and precisely apprehend criminals becomes crucial. The investigation is quicker and more effective thanks to the new law. This legislation also enables the investigating authorities to interview more people and acquire data that can be used as evidence in court. Additionally, it should be mentioned that, in terms of accessibility and communications, the entire world is getting smaller with time. In this environment, modernizing the investigations is necessary because it has become simpler to escape and conceal from the authorities.

The bill serves an essential concern of the executive in investigating and finding the truth but it poses a major threat to the right of privacy of an accused because the Bill permits executive authorities to get signatures, handwriting, or any other form of inspection allowed by Sections 53 or 53A of the Code of Criminal Procedure, 1973. The sovereign as a result may rule in a power-centred manner. The citizens of India suffer from a lack of personal space, which is a serious problem. Giving public servant officials access to biometric data is against their right to privacy. Social and political life systems may become corrupt due to the government exercising absolute control. According to the rule of law, it is the sovereign's responsibility to protect against any form of violation of a citizen's human rights. The creation of a historic record of the repeat offenders using this Bill may be helpful to the authorities in maintaining records. However, it may also violate the rights of detainees who have been charged with a crime but have yet to be found guilty by a court of law.

The Court significantly broadened privacy rights as discussed in the *Maneka Gandhi v. Union of India judgment*.[2] The approach was to use judicial construction to broaden the scope and application of fundamental rights rather than to dilute their intent and significance. Lawmakers and decision-makers should conduct thorough empirical research on the rulings rendered by the various High Courts and Supreme Courts. The 2022 CrPC Amendment Bill must be written in line with orders, constitutional principles, and human rights. All citizens, including inmates found guilty or imprisoned, will now have basic freedom. To set the objectives of liberty, equality, and freedom, a thorough and effective evaluation of the Bill is required.

[1] State Of U.P vs Ram Babu Mishra, 1980 AIR 791, 1980 SCR (2)1067.
[2] Maneka Gandhi v. Union of India, (1978) 1 SCC 248.

The article critically analyses the current bill in light of the right to privacy and the right to be forgotten which are recognised by the Indian Supreme Court as an extension to Art. 21 and highlights the loopholes in the present act and rules for its effective implementation.

EMERGENCE OF "RIGHT TO PRIVACY" IN AMERICAN JURISPRUDENCE

The right to privacy is the most crucial right protected by the U.S. Constitution, despite never being explicitly mentioned in their constitution and has played an important role in shaping U.S. jurisprudence. The history and emergence of the right to privacy in the US date back to the late 19th century and have since undergone several significant changes.

EARLY VIEWS ON PRIVACY

The early legal framework of the United States had no specific language regarding privacy rights. Most legal scholars believed that individual privacy was not mentioned in the Constitution because the founding fathers believed it to be a natural right. However, several legal scholars noted that few amendments to the American Bill of Rights could be interpreted as providing for privacy rights, like protecting against illegal searches and seizures,[3] and protecting an individual from being a witness against himself.[4]

After the 1850's cases dealing with privacy issues began to emerge. One such case was Warren and Brandeis's 1890 Harvard Law Review article titled, *"The Right to Privacy."*[5] Here, they argued that *"the common law system should recognize the right to privacy as a basic human right."* This book claimed that an individual is entitled to demand the protection of their privacy due to the increasing spread of photographic technology, which could easily capture private moments.

THE EMERGENCE OF PRIVACY IN US JURISPRUDENCE

During the early 20th century, the legal framework around privacy began to develop. Courts began to recognize privacy as an established right in American law. However, privacy was typically framed as a right to be free from unreasonable searches, rather than a more general right to privacy.

The case of Olmstead v. United States,[6] marked a turning point in the development of privacy rights. This case was significant because it involved wiretapping in a private home. The defendants argued that the evidence gathered through the wiretap was inadmissible because it violated their privacy rights. In a 5–4 decision, the Supreme Court ruled that wiretapping did not violate the Fourth Amendment because it did not involve a physical search or seizure.

In 1965, the Supreme Court went further to expand privacy rights with *Griswold v. Connecticut.*[7] In this case,

[3] U.S. Const. amend. IV.
[4] U.S. Const. amend. V
[5] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harvard L.R. 193, (Dec. 15, 1890).
[6] Olmstead v. United States, 277 U.S. 473 (1928).
[7] Griswold v. Connecticut, 381 U.S. 479 (1965).

"*the Court struck down a Connecticut law that prohibited the use of contraceptives. The Court found that the right to privacy is implied in the Constitution, and restrictions on contraception violated this right. The Court reasoned that the right to privacy came from the First, Fourth, Fifth, and Ninth Amendments*."[8]

THE ROE V. WADE CASE ANALYSIS

The most important privacy case in U.S. history was *Roe v. Wade (1973)*.[9] The case was about the right to privacy and a woman's right to choose an abortion. The Court reasoned that "the due process clause" of the 14th Amendment provided a constitutional right to privacy, which included the right of a woman to choose an abortion. The Court prohibited the action of the state and held that they could not prohibit and penalise abortion within 12 weeks of pregnancy. Roe v. Wade represented a significant shift in legal reasoning around the issue of privacy. Similarly, in 1986, the Supreme Court heard *Bowers v. Hardwick*,[10] where the constitutionality of a Georgian law was challenged as it criminalised sodomy. The Supreme Court upheld the law, stating that the Constitution did not specifically recognize a right to engage in consensual homosexual acts. The decision in Bowers v. Hardwick was overturned in 2003 by *Lawrence v. Texas*.[11]

Currently, The Privacy Act of 1974 governs how government agencies handle Americans' personal information. The statute mandated that agencies secure records, keeping them secure unless the person in the record expressly authorised any extra usage. People also have the right to view and correct information contained in federal agency records about them. The Privacy Act of 1974 contains several exemptions, including those for simple statistics purposes like the U.S. Census and more serious law enforcement purposes. There are also de facto exemptions because of the large number of documents stored outside of technical *"agencies,"* such as those of US courts.

The right to privacy has undergone considerable evolution in the United States. The precise boundaries of the right remain hotly debated, however, the Supreme Court has recognized it as an integral part of our constitutional framework. The history of privacy in American law shows a steady expansion of the right, from its origins as a principle of common law to its explicit incorporation in the Bill of Rights and the 14th Amendment. While the exact contours of the right to privacy remain contested, it is clear that it is a crucial aspect of American constitutional jurisprudence.

[8] *ibid*
[9] Roe v. Wade, 410 U.S. 113 (1973)
[10] Bowers v. Hardwick, 478 U.S. 186 (1986).
[11] Lawrence v. Texas, 539 U.S. 558 (2003

THE BACKGROUND AND EVOLUTION OF THE RIGHT TO PRIVACY JURISPRUDENCE IN INDIA.

The right to privacy as a fundamental right has been recognized globally. It is a right that protects individuals from arbitrary and unjustified interference in their private lives. In India, the right to privacy has a rich history, dating back to the early 20th century. The right to privacy in India is not explicitly mentioned in the Constitution. However, it is an integral segment of part III of the Indian Constitution.

The right has had its root in India since the early 20th century, the case of *M.P. Sharma v. Satish Chandra*,[12] was the first case where the right to privacy was discussed. The case involved a search and seizure of documents from the office of a newspaper publisher in Delhi. The publisher challenged the search alleging it was a violation of his right to privacy. The Supreme Court held that the Indian Constitution did not explicitly guarantee this right and held the search was constitutional. However, they recognized this right as part of personal liberty.

In 1962, the case of *Kharak Singh v. State of Uttar Pradesh*,[13] was another landmark case that addressed the right to privacy in India. Here the constitutionality of police surveillance of a suspected criminal was challenged. The court recognized this right as inclusive of the privilege to be left alone, and to control any dissemination of information about oneself and recognised the relevance of physical privacy.

Another important case that dealt with privacy was the case of *Govind v. State of Madhya Pradesh* in 1975.[14] In this case, the SC held privacy as a fundamental right embodied in the Indian Constitution, but it was not an absolute right. Further, there needs to be a balance between privacy and other rights, like articles 19 and 21. In 2017, the Supreme Court of India delivered a historic judgement in the case of *Justice K.S. Puttaswamy (Retd.) v. Union of India*.[15] The case challenged the constitutionality of the Aadhaar scheme, which required individuals to link their biometric and demographic data to a unique identification number.

> *"The Court recognised this fundamental right and held that privacy includes the right to autonomy over personal decisions, to control the dissemination of personal information, and the right to bodily integrity. The court held that the Aadhaar scheme was constitutional but subject to certain limitations to protect the right to privacy."*[16]

THE NEW DIMENSION OF THE RIGHT TO BE FORGOTTEN IN INDIA

This new concept owes its origin to the emergence of the digital age. It refers to an individual's right to get their private information removed from the internet or public sources. This right has been recognized in the European Union (Spain) and other jurisdictions around the world. This is a complex issue in India as we have no specific law or regulation that explicitly recognizes the right to be forgotten. However, there have been

[12] M.P. Sharma v. Satish Chandra, 1954 AIR 300.
[13] Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295
[14] Govind v. State of Madhya Pradesh, 1975 SCR (3) 946
[15] K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1
[16] *Ibid.*

several cases in this regard. One of the most notable cases is the landmark 2017 Supreme Court judgement of *Justice K.S. Puttaswamy*.[17], here this right was recognized as a fundamental right and laid the foundation for the recognition of the right to be forgotten in India.

Following the Puttaswamy judgment, a judicial trend has developed where several cases on this right have been discussed by the honourable courts. In a 2014 case of *Google Inc. v. Visaka Industries Limited*,[18] where the petitioner sought the removal of search results that allegedly defamed the company. The Delhi High Court directed Google to remove the search results but did not recognize this right.

In 2016, the Delhi High Court in *Gaurav Sureshbhai Vyas v. UOI & Ors*.[19] recognized the need to balance the right to privacy with the right to access information. The petitioner was seeking the removal of a video that allegedly showed him in a compromising position. The court while upholding the petitioner's right to privacy, they also recognized society's right to have access to such information. The court directed the removal of the video from a particular website but did not order its removal from other websites or search engines.

In 2017, the Madras High Court in *S. Muthukumar v. The Inspector of Police*,[20] gave recognition to the "right to be forgotten". The petitioner was seeking the removal of his name and photo from a news article about a criminal case in which he was acquitted. The court upheld the petitioner's claim of right to privacy, thus, any publication of his name and photo violated that right. The court directed the removal of the petitioner's name and photo from the news article and ordered the newspaper to publish a corrected version of the article without the petitioner's name and photo.

This concept was further discussed in *Sri Vasunathan v. Registrar General*,[21] Here, the petitioner requested the court to remove the name of his daughter from the copy of the judicial order and various search engines. The father claimed that his right to privacy had been violated since private information about his daughter was posted on a public platform leading to injuries to his reputation in society.

Despite the emerging jurisprudence on the right to be forgotten, there are several challenges in implementing this right in India. One of the significant challenges is the lack of clarity on how the right to be forgotten would be enforced. There is no designated authority or mechanism to regulate the removal of personal information from the Internet. It is also unclear how to balance the right to be forgotten with Article 19.

[17] *Ibid.*
[18] Google India Pvt. Ltd. v. Visaka Industries (2020) 4 SCC 162
[19] Gaurav Sureshbhai Vyas v. UOI & Ors, WP (PIL) NO. 191 of 2015.
[20] S. Muthukumar v. The Inspector of Police, CrlOP(MD)No.6279 of 2017.
[21] Vasunathan v. The Registrar General, 2017 SCC OnLine Kar 424.

NEED FOR TECHNOLOGICAL ADVANCEMENT IN INVESTIGATION AND IDENTIFICATION

"Crime Has Been Changing, and Police Agencies Need to Catch Up"

- Chuck Wexler

In India, there is a change in the way that criminals use technology to come up with new types of crimes and new ways to conduct old ones. When they discover how simple it is to peddle narcotics or steal thousands of dollars without ever having to encounter a victim face-to-face, people who have never committed crimes before get enticed. The majority of organisations have not yet started the process, therefore police departments will need to make considerable changes to accommodate these developments. In addition to training its officers and detectives on new techniques, police agencies may need to reorganise their internal structures in some cases. The field of law enforcement in India has witnessed significant changes in recent years with the advent of new technologies. These advancements have played a crucial role in enabling police departments to adopt more efficient investigation and identification techniques, thereby enhancing their effectiveness in solving criminal cases.

One of the most significant challenges faced by police departments in India is the difficulty in identifying suspects in criminal cases. Traditional methods of investigation such as witness statements, physical evidence, and circumstantial evidence have limitations, and it is often challenging to find a conclusive link to the crime. This is where new technologies come into play, offering innovative and efficient ways to gather and analyse evidence.

One of the most important technologies that have transformed police investigations in India is the use of forensics. The field of forensic science has seen rapid advancements in recent years, and DNA analysis has become an essential tool in identifying suspects and linking them to crimes. DNA analysis can provide conclusive evidence that can be used to exonerate innocent suspects and convict the guilty ones. Other forensic technologies such as fingerprint analysis, ballistics, and document analysis have also played a crucial role in solving criminal cases.

Another area where new technologies have played a critical role is surveillance. CCTV cameras have become ubiquitous in Indian cities, and they have played a crucial role in identifying suspects and tracking their movements. Facial recognition software has also become increasingly popular, enabling police departments to identify suspects in crowds and track their movements. The use of drones has also become widespread in high-security areas, where they can be used to monitor suspicious activity from a safe distance.

Social media has emerged as another crucial tool in police investigations in India. With the rise of social media, criminals are now more likely to leave a digital trail of their activities, which can be used by the police to identify suspects and gather evidence. Social media platforms like Facebook, Twitter, and Instagram have become important sources of evidence in criminal cases, particularly in cases involving cybercrime and online harassment.

In addition to the above technologies, the use of artificial intelligence (AI) has also become increasingly popular in police investigations in India. AI algorithms can be used to analyse large datasets of information and identify patterns that may be relevant to a particular case. For instance, AI algorithms can be used to analyse phone records, financial transactions, and other data to identify suspects and uncover criminal networks.

Finally, the use of mobile technology has also transformed the way police investigations are conducted in India. Mobile phones have become an essential tool for police officers, enabling them to access information on suspects, communicate with each other in real-time, and even track suspects using GPS technology. Mobile apps have also been developed to help police officers file reports, manage evidence, and track cases.

In conclusion, the need for new technologies in police investigation and identification in India is crucial. Traditional methods of investigation have limitations, and it is often challenging to find a conclusive link to the crime. The use of new technologies such as forensics, surveillance, social media, AI, and mobile technology has transformed the way law enforcement operates in the country. These technologies have enabled police departments to adopt more efficient investigation and identification techniques, resulting in a higher success rate in solving criminal cases.

INTRODUCTION TO CRIMINAL PROCEDURE IDENTIFICATION ACT 2022

The 2022 Act broadened the definition of measurements to include "fingerprints, palm prints, footprints, photographs, iris and retina scans, physical samples, biological analyses, behavioural traits like signatures and handwriting, as well as any other examination referred to in Sections 53 or 53A of the Code of Criminal Procedure, 1973."[22]

The 2022 Act allows measurements to be taken from criminally charged individuals as well as those who have been arrested or placed in preventative detention.[23] Police and prison officials have the authority to compel someone to provide measurements under the 2022 Act.[24] An order directing someone to take action in support of an investigation or process under the CrPC may be issued by a Magistrate under the 2022 Act.[25] But, section 3 makes an exception to this general rule for people who have been arrested and forbids the taking of their biological samples unless the crime was committed against a woman, a child or someone who would receive a sentence of seven years or more in prison.

The 2022 Act gives NCRB the power to compile, store, safeguard, and ultimately remove all data stored. Any law enforcement agency may request these records from the NCRB.[26] The information collected will be electronically or digitally in the record for 75 years.[27] The record of measures so collected will be destroyed if a person is not found guilty or is released without a trial; however, a court or magistrate may order the

[22] Section 2 (1)(b), The Criminal Procedure (Identification) Act, 2022 No. 11, Act of Parliament, 2022 (India).
[23] Section 3, The Criminal Procedure (Identification) Act, 2022 No. 11, Act of Parliament, 2022 (India).
[24] Section 6, The Criminal Procedure (Identification) Act, 2022 No. 11, Act of Parliament, 2022 (India).
[25] Section 5, The Criminal Procedure (Identification) Act, 2022 No. 11, Act of Parliament, 2022 (India).
[26] Section 4 (1), The Criminal Procedure (Identification) Act, 2022 No. 11 Of Act of Parliament 2022 (India).
[27] Section 4 (2), The Criminal Procedure (Identification) Act, 2022 No. 11, Act of Parliament, 2022 (India).

preservation of information in such cases if they do so with written justification.

According to the 2022 Act, it is unlawful to obstruct or refuse to allow someone to take measurements and is punished and sanctioned by imprisonment for up to three months and a fine of up to 500 rupees, or a combination of both.[28] Under the 1920 Act, State governments were given the power to make regulations governing criminal investigations; however, the 2022 Act gives both the Central and State governments the same authority to make regulations.[29]

CRITICALLY ANALYZING THE NEW ACT IN LIGHT OF THE RIGHT TO PRIVACY The current law has significantly widened the scope of the 1920 Act. Measurements are described in Section 2(1)(b) of the Bill,

"fingerprints, palm prints, footprints, photos, iris and retina scans, physical and biological samples and their analysis, behavioural characteristics like signatures and handwriting, or any other examination referred to in Section 53 or Section 53-A of the CrPC 1973."

The lawmakers aim to make measurement exclusive by including a collection of all terms like physical and biological samples, which could result in the use of unnecessary force thereby directly violating Articles 20(3) and 21 of the Indian Constitution. A further process like narcoanalysis and brain mapping can always be used behind the veil of *'collecting samples.'*

Indian Constitution's Article 20(3) aims to protect individuals from self-incrimination but due to this legislation, this right is also in danger. Additionally, it violates the United Nations Charter's provisions on human rights. Furthermore, the period for keeping the record is 75 years which in itself is a long time and is a blatant infringement of the right to erasure as acknowledged in the *K S. Puttaswamy case*.[30] Additionally, it violates the very principle of justice i.e. *"a person is innocent until and unless he or she is proven guilty in a court of law."* In the Maneka Gandhi case,[31] the Court expanded the interpretation of Article 21 by including in its definition of "the right to life" both the physical right to live and the psychological right to live with inherent human dignity. A person's life is put on hold by this act because he will constantly be monitored by the government, which is invading his privacy. *State of Andra Pradesh v Challa Ramakrishna Reddy*.[32] The court decided that-

"everyone is entitled to the right to life as a fundamental human right. It is so fundamental that nobody, not even the government, has the right to break it. A person retains their humanity even when they are in prison. Due to his continued human status, he is still entitled to all fundamental rights, including the right to life."[33]

[28] Section 6, The Criminal Procedure (Identification) Act, 2022 No. 11, Act of Parliament, 2022 (India).
[29] Section 8, The Criminal Procedure (Identification) Act, 2022 No. 11, Act of Parliament, 2022 (India).
[30] Supra Note 15.
[31] Maneka Gandhi v Union of India, (1978) 1 SCC 248
[32] State of A.P. v Challa Ramakrishna Reddy, (2000) 5 SCC 712
[33] *ibid*

ISSUES AND CHALLENGES OF THE NEW 20222 RULES.

The terms 'analysis,' 'biological samples,' and 'behavioural attributes,' used in the defining measurements, lack a fixed meaning, making it a subject interpretation giving rise to the possibility of infringement of Article 20(3).[34] Further, resisting or refusing to allow taking measurements is illegal according to the 2022 Act and is punished under section 186 of IPC.[35] The right to life and liberty guaranteed by the Indian Constitution are both violated by this type of criminalization. It also violates the individual's right against self-incrimination. By allowing a Magistrate to issue an order requiring anyone to provide measurements, the 2022 Act grants discretion to the provider of the reason. The Indian Constitution further guarantees citizens the right to be free from arbitrary and unreasonable state action, and this action violates that fundamental principle.

A person accused of a minor offence is treated similarly to a heinous offender under the new act because it does not distinguish between accused individuals according to the seriousness of the offences committed.[35] The 2022 Act mandates that the NCRB maintain records, but it makes no provision for how those records will be generated or maintained. Data security methods and the way that records will be shared are also distinctly unclear. The 2022 Act invites power abuse by giving authorities the discretion to extract measurements *"if so required."*

Conflicts between Centre - State authorities are also a major challenge in the new act as both the government have the authority to pass legislation. *"The collection, storage, processing, sharing, and destruction of measurements"* are not addressed in the 2022 Act or rules. The measurements according to the act will be taken by either a police or a prison officer who is authorised to do so by the government and has access to the database maintained by NCRB. But according to the Rules, this is expanded to include not only registered medical professionals but also individuals who are authorized in this capacity and anyone skilled in taking measurements.[36] Thus, by including these other categories of people that are not mentioned in the Parent Act, the Rules are overstepping their scope. Further, Neither the act nor the rule defines an expert who is eligible to take measurements.

The NCRB is empowered by the Act to gather, store, process, share, and destroy measurement records and the act grants the national and state governments the power to enact laws.[37] The rules However state that the NCRB will develop policies and procedures for measurements, its handling and storing, process, matching and removal, etc through SOPs.[38] Two issues are raised by this.

The Rules transfer rule-making authority to the NCRB, which is a case of excessive delegation. In 2014, the Supreme Court observed that *"Subordinate legislation, which is generally in the realm of Rules and Regulations dealing with the procedure on implementation of plenary legislation, is generally a task entrusted to a specified authority. The Legislature has chosen to assign the responsibility to an agency because it does*

[34] Section 2 (1) (b), The Criminal Procedure (Identification) Act, 2022 No. 11, Act of Parliament, 2022 (India).
[35] Section 6(2), The Criminal Procedure (Identification) Act, 2022 No. 11, Act of Parliament, 2022 (India).
[36] Section 3, The Criminal Procedure (Identification) Act, 2022 No. 11, Act of Parliament, 2022 (India).
[37] Section 3, Criminal Procedure (Identification) Rules, 2022.
[38] Section 4, The Criminal Procedure (Identification) Act, 2022 No. 11, Act of Parliament, 2022 (India).

not need to spend time working out the specifics of how the law will be put into practice. Such a task cannot be delegated by that agency to its subordinates because doing so would be a betrayal of the delegate's confidence."[39]

This begs the question of whether or not these SOPs would be submitted to state or union legislatures for their approval. By the Act's requirements, the Rules must be presented to Parliament or state assemblies. For instance, the proposed Rules must be laid out. It is unclear, though, whether the NCRB's SOPs will be examined in this manner. These SOPs are guidelines that the NCRB will release for gathering, storing, and processing measurements. It is essential to maintain separation of powers but in this case, the organisation that is issuing the guidelines is similar to the one who needs to follow them.

According to the Act, the records will be saved, protected, and disposed of and if the individual is released without any trial or given acquittal after all appeals, their records will be destroyed. According to the rules, SOPs will outline the process for record disposal and destruction. Any record that needs to be destroyed must be requested by a nodal officer.[40] The nodal officer will advise the NCRB to destroy the records once they have been verified as not being connected to any additional criminal cases. Thus, the new rules place the burden on the individual to make such a request for such destruction, even though the Act mandates that such records are to be destroyed by the authorities.

In some other laws, it is the government authority that holds the responsibility to eliminate personal information or data which is no longer required, sometimes even the courts may order the authority to do so. For instance, In cases of juvenile offenders except for offences of heinous nature, the record of the case post-adjudication is destroyed.[41] The Juvenile Justice Board issues such orders to the police, the court, and its registry to destroy the records once the punishment is served and the juvenile is re-introduced to society.[42]

CONCLUSIONS

Finally, privacy is a fundamental right that every person should have. Any violation of this right can have serious consequences in people's lives. In India, privacy violations have far-reaching consequences ranging from emotional trauma to financial loss and even physical harm. Cybercrime, identity theft, stalking, and surveillance are just a few examples of how privacy is violated in India.

Individuals are not the only ones who suffer from invasions of privacy. The government and other organisations must also accept responsibility for their actions that may violate people's privacy. Many people breathed a sigh of relief when laws like the Right to Privacy Act of 2017 were passed, which prohibited any unauthorised interception or monitoring of communication. However, the challenge remains in enforcing such laws to ensure that they protect citizens from any form of infringement.

[39] Section 3(2), Criminal Procedure (Identification) Rules, 2022.
[40] Siddharth Sarawagi vs Board of Trustees for the Port of Kolkata and others, SPECIAL LEAVE PETITION (CIVIL) NO.18347/2013, Supreme Court of India, April 16, 2014.
[41] Section 4, 5, Criminal Procedure (Identification) Rules, 2022.
[42] The Juvenile Justice (Care and Protection of Children) Model Rules, 2016, Ministry of Women and Child Development, September 21, 2016.

To summarise, the consequences of infringing on the right to privacy in India are serious and varied, made more so by the passage of the new criminal procedures (identification) Act. The loss of personal data or the fear of data leakage can have serious emotional and financial consequences in people's lives. As a result, both individuals and organisations must take the necessary precautions to safeguard private information.

The present act is made with a positive intent i.e. to enhance current prisoner identification methods and increase the effectiveness of the investigative process. But still, there are a few provisions which lack clarity and thus it drew scathing criticism for being overbroad, disproportionate, and violative of the right to privacy, the period of 75 years is a huge duration thus raising issues with data privacy also. Data security is also an issue, while the act only mentions storing and destroying the data so collected, there is no penalty in case there i some breach of data. The current act and rules need to be critically analysed by the judiciary to ensure its constitutionality and the legislature must amend the law to clear various ambiguities in defining the terms mentioned in the current act and adequately reframing the provisions on destroying and saving data of the current act.