THE CRIMINAL PROCEDURE (IDENTIFICATION) BILL, 2022: A PATH TOWARDS A FAIR AND SPEEDY TRIAL?

Shrrijiet Roychowdhary*

ABSTRACT

Biometrics and forensic science have been deeply influenced by Locard's exchange principle which established that a perpetrator of a crime will bring something into the crime scene and leave with something from it, and that both can be used as forensic evidence. Investigating agencies in India have often lacked proper resources and support to collect substantive and corroborating evidence which can help the prosecution build a case. The Criminal Procedure (Identification) Bill, 2022 takes a leap forward in assisting investigation agencies in India in collecting and storing biometric information and competing with the developed nations over matters of criminal investigation and border control. This article talks about the legislative intent of the bill and highlights the current criminal investigation fallacies of the country. The bill talks about the scientific and technological advancements made by other developed countries in the field of investigation and border management and strikes a comparison to signify the true meaning and intent behind the Bill. The article also talks about the legal obstacles and the contentions raised by the opposition parties in the Lok Sabha and counters their arguments based on precedent cases.

Keywords: Biometrics, Criminal, Investigation, Forensic, Privacy.

INTRODUCTION

The Indian Home Minister on March 28, 2022, introduced the Criminal Procedure (Identification) Bill, 2022 as a part and parcel of the series of efforts made by the government for speeding up the trial and justice system in our country. This bill has been the victim of controversy either by those following a different political agenda or by human rights activists on grounds of severe infringement of the right to privacy and misuse of such data by the police authorities. This bill takes a step forward in modern criminal investigation by helping in the identification process during the investigation and assists the entire process of the police.

*LLB, OP JINDAL GLOBAL UNIVERSITY, SONIPAT.

What kind of data does the Bill aim to record?

The Bill authorizes the collection of "measurements" defined under Section 2(1)(b) which include finger- impressions, palm-print impressions, foot-print impressions, photographs, iris and retina scan, physical and biological samples and their analysis, behavioral attributes including signatures and handwriting, or any other examination referred to in Section 53 or Section 53A of the Code of Criminal Procedure, 1973.

To whom does the Bill pertain?

Section 3 of the bill engineers a greater expanse of the ambit of the term "any person" against whom such rights can be exercised, and those include:

(a) Convicted of an offence punishable under any law for the time being in force; or

(b) Ordered to give security for his good behavior or maintaining peace under section 117 of the Code of Criminal Procedure, 1973 for a proceeding under section 107 or section 108 or section 109 or section 110 of the said Code; or

(c) Arrested in connection with an offence punishable under any law for the time being in force or detained under any preventive detention law .

Who possesses the right for collection, storage and preservation of such data?

The Home Ministry entrusted the sole right to store, preserve, destroy, process, share and disseminate such information to the National Crimes Record Bureau (NCRB). The government has given a huge expanse to the law-enforcing agencies to exercise their duty to collect such data and further report them to the relevant authorities. The aim of the collection of such data by the NCRB is to create a national-level platform that can be used only by the relevant authorities and cannot be scrutinized or accessed by local-level police authorities. The Bill mentions the combined effort of the State and Central government who by notification of the Official Gazette shall provide for the procedures for collection and sharing of such data and further dissemination, destruction, and disposal of records.

Detail analysis of the Bill

The Bill adds some required definitions to the Code of Criminal Procedure which includes the definition of 'Magistrate' to include within its ambit the different kinds of Magistrate

based on their area of jurisdiction. Further the Bill, according to its requirements defines 'measurements' considering the seismic shift in the collection of data of prisoners and persons in arrest for certain crimes. The Bill includes the definition of 'police officer', 'prescribed', and 'prison officer' which are important definitions in terms of the personnel who have the right to collect or access data that are highly sensitive to the country's criminal database.

Clause 3 of the bill specifies the ambit under which law enforcement authorities are authorized to take measurements as defined above of individuals falling under the three categories mentioned for the sake of identification and investigation in criminal circumstances. The amendment adds a proviso stating that besides the three instances where biological and physical samples have to be given, no person arrested for an offence committed under any law for the time being in force (except for an offence committed against a woman or a child or for any offence punishable with imprisonment for a period not less than seven years) may not be obliged to allow taking of his biological samples under this provision.

Clause 4 of the Bill gives the right to store, preserve and destroy records to the National Crime Record Bureau of all the concerned persons but at the same time, adds a proviso stating that a "person who has not been previously convicted of an offence punishable under any law with imprisonment for any term, has had his measurements taken according to the provisions of this Act, is released without trial or discharged or acquitted by the court, after exhausting all legal remedies, all records of measurements so taken shall unless the court or Magistrate, for reasons be recorded in writing otherwise directs, be destroyed from records".

Furthermore, clause 5 of the Bill gives the right to the Magistrate to direct any person to give measurements for the purpose of investigation and the refusal to give such measurements as mentioned under clause 6 of the bill would amount to an offence of Section 186 of the Indian Penal Code. Under this section, a person shall be punished with imprisonment of three months or a fine of five hundred rupees or both.

Clause 7 of the Bill imposes a bar on any kind of legal action against any person which could have happened to have been intended to be done in good faith. Clause 8 of the Bill on the other hand divides the work of issuing directions for carrying out these purposes between the State and the Central Government. The Centre and the State should together formulate rules

for (i) how to take measurements and (ii) the manner of collecting, storing and preserving those measurements and also sharing, disseminating, destroying and disposing of those records. Clause 8(3) states the procedure to be followed by the Central Government in the formulation of the rules. The Amendment makes it clear that every rule has to be placed before both Houses of the Parliament and if both Houses agree to have a modification in the rule or that the rule should not be made, then the rule thereafter shall effect along with the modification of no effect at all.

Clause 9 of the Bill helps tackle any kind of difficulty arising from the provisions of the Act, the Central Government may by order make such provision inconsistent for removing any kind of difficulty. Following that, the amendment repeals the Identification of the Prisoner's Act, 1920 , and invalidates any action under that law taken against any person.

INTERNATIONAL COMPARISON

The United State of America

The United States has been a leader in conducting biometrics identification to strengthen its ability to not just combat crime and terrorism but also as simply as granting a US visa to its travelers. The Office of Biometric Identity Management under homeland security makes the priority of biometrics to be primary as it supports national security priorities and ensures delivering accurate, timely and high-assurance biometric identity. The three modalities availed by homeland security for biometric identification are fingerprints, facial recognition and iris scans. This service of biometric identifiers has domestic and international sharing facilities which are mainly utilized for borderland security where they can be used by international partnerships to share information on lost and stolen passports, sharing biometrics with international partners seeking information on wants, warrants, or lookouts. India is a country with multiple land border neighbors with whom it shares an acute problem of border disputes for years, this becomes a plausible way of handling its border security and sharing vital data with its neighboring countries.

The Federal Bureau of Investigation (FBI) trains individuals for collecting and measuring biological data and behavioral characteristics like fingerprints, DNA, iris scan, voice pattern, plan prints and facial patterns. The Bureau to harness new technologies and improve identifications has developed its Next Generation Identification (NGI) system which provides

the criminal justice community with the world's largest and most efficient repository of biometric and criminal history information.

In terms of international cooperation, the US has also opened up an opportunity to take a step forward in initiating the Foreign Biometric Exchange (FBE) program which comes with the primary mission to collect high-value biometrics from partner nations which would help in the combined efforts of identifying terrorist activity, egregious crimes and transnational criminal activity. The FBI preserves submissions taken from fingerprints also known as a "rap sheet" which are obtained from arrests and in some instances federal employment or military services and saved in a machine-readable format. This system is difficult to be breached by hostile forces and cannot be deceived by forged paperwork or stolen uniforms. The same technology was proved to be extremely advantageous in the U.S. military's playbook in Afghanistan where they used the Handheld Interagency Identity Detection Equipment (HIIDES)to create a database not just for the servicemen for the mission but also for potential threats, checking individuals on watch lists and identification of rebel groups. Though the main objective of the bill cannot be the same approach as that used in a warzone maintaining a system with a proper threshold can surely be a boon in disguise for the future.

The United Kingdom of Great Britain& The European Union

The United Kingdom has optimally utilized the biometrics system in solving its immigration crisis and has incorporated that in its investigation procedures quite often. The Scottish Parliament has already determined that it does not view police use of biometrics as a matter of data protection. The National DNA Database (NDNAD) Statistics as of 31st March 2022 holds all the current police fingerprint databases in England and Wales established in 1995 which holds a total of 6.8 million crime scene sample profiles. There the system of accessing and utilizing such data is more unrestricted as police officers in South Wales Police use the system of Operator Initiated Facial Recognition to confirm the identity of a wanted suspect without the need to go back to a police station. Though it is not so that the powers of the police are unnoticed and unlimited. The Office of Biometrics Commissioner (OBC) made by chief police officers is entrusted with determining whether the police have the power to retain an individual's biometrics after reviewing all National Security Determinations (NSDs).

As a part and parcel of the effort for an integrated biometric service provision, the UK government has announced the One Login for the government program, where a step ahead

has been taken to eliminate duplicated digital ID accounts and cut down around $ 1.2 billion from the central government's cost.

Similarly, the European Union has already taken a step forward in outsourcing biometric data to the private sector where they are being used for targeted marketing, medical diagnostics, and by law enforcement and border control authorities. The European Union has a handful of laws that lawfully grant the power to collect, store and share biometric data for border control and security. The Entry-Exit System Regulation (EES Regulation) is one of the standing examples of the European Commission's Smart Border Package. These centralized data banks are for handling mass people crossing the borders of Member nations and comparing the fingerprints of asylum applicants. This kind of data remains highly sensitive and receives the protection of the European Commission of Human Rights which lays down proper guidelines for these procedures.

Biometrics the need of the hour

Criminals engage in all kinds of forgery to doge police and law enforcement agencies. They change looks, and places, manipulate or fake identities, counterfeit documents, etc which do not require much effort because of the use of technology. The criminal justice system, especially in India requires quick action and quicker identification of people, especially suspects and criminals.

Cyber security is one of the main concerns of the world and has attracted the attention of countries in cyber security laws. The expanse of cybercrime has recently increased as it not just includes sexual, racial, religious, or any other kind of harassment towards an individual or a group but also against property and organization like computer wreckage, transmission of harmful programs and unauthorized possession of computer information and against the government which can amount of cyber terrorism. According to the FBI's reports, India ranked for a second time on the list of global cybercrime victims in 2020. FBI Deputy Director Paul Abbate stated in the report that "Cyber incidents are in fact crimes deserving of an investigation, leading to judicial repercussions for the perpetrators who commit them".

The present-day fingerprint recognition methods leverage a unique pattern that cannot just be utilized in the investigation but also to check civil identification, employment background and management of biometric data. It can be used for the reliability of one's testimony and to assure whether one's a hostile witness or not. In the same way, facial recognition have been a

very popular method recently and just like fingerprints have been a source of identification in the simplest of devices like our smartphones.

DNA profiling has in the past and in the present helped law enforcement agencies solve complex cases in which there was no other strong evidence. The best case supporting this claim is the 1984 Melanie Road murder case in which the man responsible for killing a 17-year-old girl was jailed after 32 years because of the lack and evidence which led to the police authorities matching her DNA data through the national database to find her killer. There are a plethora of cases where the evidentiary value of DNA has been given the highest value and based on which a conviction or an acquittal has been based.

Biometric identification has already been a success in Maharashtra where the Mumbai Police in 2019 stored 6.5 lakh fingerprints of criminals dating from the 1950s onwards. The Automated Multi-modal Biometric Identification System (AMBIS) was a success for the investigation teams during the one-year testing period since it was introduced. It was reported that the AMBIS was linked to the CCTV system to identify the faces of suspects and offenders, and with the Crime and Criminal Tracking Network and System (CCTNS)- a digital tool to aid investigations and detection of crime.

APPLICATION IN CRIMINAL INVESTIGATION& LEGAL ANALYSIS

The amendment has made a strong standing in making crime detection easier. The Home Minister in his rebuttal to the Lower House stated that the assertion of misuse of the proposed law cannot be a reason to not implement the law. The opposition had raised where the right to life and right to privacy of an individual has been contested to be violated on two instances in the amendment, firstly, on the collection of private data and secondly, on criminalizing the refusal to provide such data to the relevant authorities.

S & Marker v. UK (2008)

In the ongoing deliberation, the case of S & Marker v. UK (2008) in the European Court of Human Rights finds high relevance in defining the validity of such legislation. In this case, the applicant's fingerprints and cellular samples were acquired on an attempted robbery case for an indefinite period even after the acquittal of the accused in trial. During the trial of the case, the UK was one of the only countries that had provisions for the permanent retention of sensitive DNA profiles acquired from crime scenes and otherwise as well. In this case, the

applicants submitted that the statistics presented by the respondents on displaying sufficient relevant reasons for recording such data were misleading and thus could not continue with such an indefinite right. The court thus acknowledged the infringement into the applicant's private life given the wealth of genetic information contained therein. The court stated that "mere retention and storing of personal data by public authorities, however, obtained, are to be regarded as having direct impact on the private-life interest of an individual concerned, irrespective of whether subsequent use is made of the data".

It comes with astute observation of the case and why the court passed such a verdict. It is important for us to consider the present facts and conditions on which the bill will hold more water considering the present requirements of criminal investigation. Two decades ago, in the United Kingdom, besides legislation stating provisions for recording such data, there were no regulatory authorities and no rules and regulations to keep their actions in check. Scientific utilization of the data collected for running matches in their system was not in its prime and the retention of such data whether acquitted or convicted was indefinite and not time limited. These facts added to their case and led to the verdict, but the bill passed in the Lok Sabha addressed all these issues and made clear the intent of the bill. The bill made clear a period of 75 years for which the data collected of a convicted individual will be retained, but if acquitted, will be destroyed from the government's records. The bill is supplemented by pre-existing bills to curb any kind of coercive actions like the DNA Technology (Use and Application) Regulation Bill, 2019 which waves off the consent requirement for collecting DNA collection of a person arrested for offences punishable with death or imprisonment for a term exceeding seven years. Under this bill, the National DNA Data Bank and Regional DNA Data Bank established would be maintained under different categories like (i) a crime scene index (ii) a suspects' or undertrials' index, (iii) an offenders' index, (iv) a missing persons' index and (v) an unknown deceased persons' index.

Justice K.S. Puttaswamy v. Union of India (2018)

This landmark judgement questioned the constitutional validity of the Aadhar card scheme which was introduced by the Union government. The petitioners in this case contested that the collection of demographic data by the government was an infringement of their right to privacy. The Apex Court in this case gave recognition to the right to privacy and overruled the previous cases of M.P. Sharma and Kharak Singh where the court did not find the right to privacy under the ambit of the constitution. In this case, the court stated that definitional

uncertainty is no reason not to recognize the existence of a right to privacy. It gives every person the right to self-determination, liberty, autonomy, and liberty which are all interconnected and equally important under the Right to life guaranteed under the Constitution.

While providing rights to the citizens, the courts gave the duty of data regulation and protection to the government and stated that laws enacted must justify the encroachment on the privacy of an individual which must be reasonable and non-arbitrary in its nature. In the judgement of Maneka Gandhi , the court stated that the law would be assessed not with reference to its object but on the basis of its effect and impact on fundamental rights. This case laid down laws to be tested on the basis of their fairness and reasonableness in determining whether the 'procedure established by law' must pass under Article 21. This notion stems from the ratios explained by the judges that the "Right to Privacy is not an absolute right, it is subject to restrictions and limitations made by the State to protect legitimate State interests or public interest". This Bill introduced in the Lok Sabha was to tackle the problems faced in criminal investigation and did not classify any group of people in the bill, thus did not have to justify itself for any kind of reasonable classification. To maintain the Right to Privacy, the Home Minister in his speech made it clear that no lower authorities or third parties will have the right to access or manage such data, it will solely be taken care of by the NCRB.

While the question of privacy is of vital importance, under section 3 of the bill, the legislature stated that for personnel who are obligated to provide their data, there is also an exemption given to personnel who are arrested for an offence (except the ones for an offence committed against a woman or a child or for any offence punishable with imprisonment for a period not less than seven years) 'may' not be obliged to provide their data. This protects people from any misuse of power by police authorities as the clause leaves it at the discretion of the people who are arrested.

Thus, under no circumstances can this law fail the test of permissible restrictions as no right can be absolute to the citizens along with the test of fairness and reasonableness laid down in the Maneka Gandhi case. Thus, the applicability of other landmarks judgements safeguarding the privacy of an individual like K. Gopalan v. State of Madras, Kharak Singh v. State of U.P., Charles Sobraj v. Supt. Central Jail, Sheela Barse v. State of Maharashtra and Pramod

Lumar Saxena v. Union of India become redundant as the state has the right to enforce law and order and no right can be absolute without the test of fairness and reasonableness.

CONCLUSION

The disadvantages of this bill did not just rely on the minimal possibility of misuse and mishappening and possible coercion which have not only been tracked up till now in the history of biometric identification systems but also lack of experience the country's authorities have in this domain and the lack of proper set-out procedures which have been ensured by the government for this bill. The reliance on such negative functionalities would limit the growth of the country towards new endeavors and not set us at par with the developing and developed nations in our system of delivering justice.