INDIAN JOURNAL OF LAW, POLITY AND ADMINISTRATION

RIGHT AGAINST SELF-INCRIMINATION AND RIGHT TO PRIVACY IN THE CONTEXT OF PERSONAL GADGETS IN THE PRESENT DIIGITAL ERA

AYUSH NEGI
(National Law University Delhi)

ABSTRACT

The right against self-incrimination and Right to Privacy enshrined under Article 20(3) and Article 21 of the Constitution of India respectively are considered as sacrosanct and their importance has been strongly emphasized in various judicial pronouncement all across the globe. At the same time heavy reliance on Smartphones and personal gadgets has created a new spark in the world. Smartphone users pay so much attention to their privacy that if some mobile application demands access to the large amount of personal information stored in their devices, then they usually refrain from using such applications. These personal gadgets provide a useful insight into the daily lives and activities and personality of an individual and thus this personal data stored in these smart devices can easily act as a fertile source of evidence against that individual. This article seeks to provide insight into relationship between right against self incrimination and right to privacy with respect to compelling the accused to give fingerprints or other biometric information to unlock Smartphones and other personal gadgets. This article argues that the information contained in Smartphones stands relevant today in this Digital age and thus can be easily be deployed against an individual coercively and therefore would violate the individual's right against self-incrimination and right to privacy.

INTRODUCTION

In present world, one of the safest assumptions a person could make is that any random person walking with his/her Smartphone. Alternatively we have become so much dependent on them that they have become the extension of ourselves. Justice Roberts, the former chief justice of America has remarked that these Smartphones have become such a insistent part of our daily lifestyle that any visitor from other planet like Mars might conclude that Smartphones were an important feature of human civilization. [1]

[1] *Riley v. California*, 134 S. Ct. 2473, 2484 (2014).

People store private information in their devices and often create back up data on their devices indicating how much value they attach to the information stored in their device. The ambit of private information is very wide differing from person to person. Mainly private information includes our text messages, pictures, videos and documents, online banking transactions. However this list is not exhaustive as private information differs from person to person. Therefore given our dependency on these smart devices, it is reasonable to conclude that people performing various activities on their smart devices attach high level of privacy with them. Thus these private activities carried on smart devices make safety and encryption of smart devices a necessity. Today, almost all the technological companies including some giant ones such as Apple or Samsung have developed advanced encryption features in smart devices, providing wide range of enhanced security features which includes pass-words, pattern, fingerprint sensors and face-id. Irrespective of which method of encryption is used, the purpose remains the same i.e. protecting our private data from third party intruders and making it inaccessible to them.

In India, number of people using smart devices such as Smartphones, laptop or tablets have numbered over 200 million in 2016.[2] Further as per Morgan Stanley report, the total number of internet users in India is expected to cross 600 million by the year 2020.[3] Now these Smartphones and devices contain so much private information about a particular individual that it can be used as crucial evidence against that individual in criminal trial. Since investigating authorities have various powers to seize these smart devices and phones of an individual in the process of their investigation, it is therefore in these circumstances, a big question arises about the constitutional rights of an individual i.e. right against self incrimination and right to privacy. Therefore it is imperative to understand the implications of such practices of investigating authorities which involves seizing of personal smart devices and then asking the individual to unlock those devices. Hence it is incumbent upon the Indian legal system to address these constitutional challenges in this era of technological advancements.

The article has been divided into two parts. The first part analyzes whether compelling individuals to give their fingerprints and other bio-metric information to unlock their smart

[2] Eslie D'Monte, *What's it with Indians and Social Networks*, LIVEMINT, May 2, 2015<< http://www.livemint.com/Consumer/HmOwoRlDsGYs9DModr1QLP/Whats-it-with-Indians-and-social-networks.html>> (last visited 27 January 2020).

[3] Id.

devices violates their right against self incrimination and it also gives an overview of position of law in U.S.A. The second part analyses whether the government's forceful invasion to the contents of the smart phones and devices violates right to privacy along with the some important case-laws of India and U.S.A.

PART-1

ISSUE OF COMPELLED FINGERPRINTS AND OTHER BIOMETRIC INFORMATION AND THE RIGHT AGAINST SELF INCRIMINATION

Investigating authorities of state while carrying out investigations has power under C.r.P.C.[4] to search and seize mobile phones, laptops and other smart gadgets. Also, the Information and Technology Act empowers the state to use personal data stored in electronic devices of an individual during the course of investigation. [5] Thus these investigating authorities have access to vast amount of personal data which can easily act as a fertile source of evidence against that individual.

Article 20(3) states that "no person accused of an offence must be compelled to be a witness against himself". Many international instruments and jurisdictions have recognized the relationship between right to fair trial and right against self incrimination. In India also after *Maneka Gandhi v. UOI* [6] which has incorporated right to fair trial under right to life, article 20(3) must be construed in light of personal liberty under article 21 of the constitution. Article 20(3) has three main components: a) a person accused of an offence b) compelled c) to be a witness against himself i.e. is the incriminatory evidences are self directed. In order to understand whether information gathered from seizure of Smartphones and device and compelling the person to unlock the information stored in these devices is in violation of article 20(3) of the Constitution, it is imperative to comprehend the three vital components of article 20(3).

a. Accused of an offence

[4] Code of Criminal Procedure1973, sec 91.
[5] The Information Technology Act, 2000, (Act 21 of 2000), s. 69, read with the Interception Rules, 2009.
[6] (1978) 1 SCC 248.

The first main element of article 20(3) is that the person must be an 'accused' of an offence. There is lack of clarity on the meaning of word 'accused' due to the absence of its statutory definition. In *Romesh Chandra Mehta v. State of West Bengal,* [7]court tried to defined accused as a one against whom an FIR has been lodged or a complaint against that person has been made to the magistrate.

This interpretation of 'accused' however can only protect individuals against whom formal accusation is made or FIR has been lodged. Thus this interpretation would exclude those cases where incriminatory statements were made prior to the filing of FIR. For example various legislations like Narcotics Drugs and Psychotropic Substances Act 1985 or Income Tax act 1961 states that statements made by the person before the formal accusations can be used later in the case. And courts also treat this phase of investigation as a "preliminary enquiry phase". [8]

Thus deploying the same rational here i.e. in cases of extracting information from Smartphone and other personal gadgets prior to an FIR being filed or formal accusations has been made is equally in violation of his right over controlling personal information and autonomy. For an instance any Income Tax Officer investigating some tax/finance related offence may access transactions of financial history stored in mobile or laptop. Similarly an officer under NDPS may find search history or conversations relating to narcotics and thus provides incriminatory information against that individual even if no FIR has been formally filed. Merely because FIR has not been filed does not equip the state to interfere with the information of an individual which he does not want to expose to third parties. Justice Krishna Iyer in *Nandini Sathpathi* [9] in this regard pointed out that denying protection of constitutional shield to a suspect merely because enquiry is preliminary in nature would indicate gross failure of constitutional values.

Hence in order to ensure constitutional safeguards, it is necessary that information derived through search and seizure of mobile or similar smart gadgets by compelling the individual to unlock these smart gadgets prior to any formal accusations shall also come within the scrutiny of right against self-incrimination.

b. Compelled

[7] AIR1970SC940.
[8] *Directorate of Enforcement* v. *Deepak Mahajan*, (1994) 3 SCC 440.
[9] *Nandini Sathpathy v P.L. Dani* (1978) SCC (cri) 236.

Compulsion in the context of criminal law can be defined as any mode of pressure subtle or crude, mental or physical direct or indirect deployed by police or investigating authority to obtain information from accused amounts to compelled testimony.

In *Oghad* [10], compulsion has been interpreted as equal to duress which refers to an act of injuring, beating or unlawful imprisonment. The Court also explained the compulsion may also be performed mentally by putting the mind in some extraneous excruciating environment. Justice Krishna Iyer in *Nandinin Sathpathy*[11] held that any investigation where police or investigating authority gives rest to fists and give restlessness to wits is considered as the best. In this regard compulsion may be interpreted as evidences procured through involuntary measures.

In the context of information gathered through Smartphones and other personal gadgets, this component of compulsion is easy to establish as any information or evidence obtained through forceful seizure and then compelling a person to unlock device or accessing the data through other unauthorized ways will definitely come under the ambit of compulsion as provided under article 20(3) of the constitution.

c. To be a witness against himself

In *M.P. Sharma*,[12] witness was defined as the one who furnishes evidence hence evidence can be furnished not only through oral medium but also by producing documents or things or in any other modes. Since art 20(3) provides protection against testimonial compulsion therefore court also defined 'testimony' as a positive volitional act which leads to furnishing of evidence. In *Oghad*[13] Justice Sinha writing for the majority judgment narrowed down the interpretation which was given in M.P. Sharma and ruled that 'witness' means imparting knowledge of relevant facts by means of oral statements or written statements. Provision of self incrimination provides protection against conveying information based upon personal knowledge. Therefore the majority judgment concluded that giving of specimens of handwriting or fingerprints impression may amount to furnishing of evidence in the larger sense but since such fingerprints impression or handwriting sample are merely physical characteristics of the body and do not convey any personal knowledge hence they do not come under the ambit of art 20(3). However in the same case Justice Dasgupta in his

[10] Supra note 11.
[11] Supra note 9.
[12] *M.P. Sharma v Satish Chandra* AIR 1954 SC 300.
[13] *The State of Bombay v Kali Kathu Oghad* AIR 1961 SC 1808 .

dissenting judgment held that even though accused is not imparting any personal knowledge but he can do so by other means such as production of documents which though do not convey any personal knowledge but still those documents may have the tendency to make a case probable against the accused. However regarding the issue of giving of handwriting samples or finger impressions, he maintained the same view as was held by the majority bench.

POSITION OF LAW IN USA

In U.S.A. also we can see the similar position of law with respect to right against self incrimination. The fourth amendment of Federal Constitution provides protection the right against self incrimination. In *Holt v. United States*[14] the court differentiated between 'physical evidence' and 'testimonial /communicative evidence' and fourth amendment protects evidence which are testimonial in nature and does not cover physical evidence like body. The same reasoning was followed in *Schmerber v. California*[15], and the court held that giving of blood samples may be a potentially incriminating evidence but it cannot attract the privilege of right against self incrimination as giving of blood samples is merely a non-testimonial and non-communicative act. However in *Hubbell*[16], the court shifted from physical and testimonial evidence to the mental element of the accused. The court ruled that compelling the accused to go through his mental contents in order to identify documents out of the hundreds of documents requested in subpoena definitely attracts the right against self incrimination clause as the mental efforts involved in assembling document would constitute a testimonial act. Following this judgment, in *In re Grand Jury Subponea Tecum*[17], it was held that compelling an individual to give computer password in order to decrypt data stored within it was a violation of right against self-incrimination as the same involves compelling the individual to go through his mental process. However in *Commonwealth v Baust*[18] Virginia trial court ruled that compelling the defendant to give fingerprints to unlock mobile phone does not requires him to divulge and go through mental process of his mind. Further giving of fingerprints is analogous to giving of DNA or blood samples and the same are equivalent of physical evidence and not testimonial /communicative evidence. Similarly in

[14] 218 U.S. 245 (1910).
[15] 384 U.S. 757 (1966).
[16] *United States v. Hubbell,* 530 U.S. 27, 43 (2000).
[17] *In re Grand Jury Subpoena Duces Tecum* Dated Mar. 25, 2011, 670 F.3d at 1352–53.
[18] *Commonwealth v. Baust*, 89 Va. Cir. 267 (20140.

State v. Diamond[19] the Minnesota Appellate Court held that compelling the person to give fingerprints does not require him to disclose his mental contents and thus do not amount testimonial compulsion.

The current legal framework maintains the position that only those acts which forces the individual to go through his mental contents or requires him to disclose his personal mental elements would amount to testimonial compulsion and according to some major verdicts of courts password is also included under the right against self-incrimination but finger prints or face-ids are not located inside the mind of a person therefore giving of fingerprints to unlock cell phones does not amount to testimonial compulsion.

But keeping aside the legal technicalities and paying due attention to the fact that the information and data stored in such smart devices like the kind of videos, music, files and documents stored in such devices also show our taste, preference or alternatively they show our mental state and as it was rightly stated in *Selvi v. State of Karnataka*[20] that no person including State must be allowed to interfere with such mental autonomy and especially in those circumstances when a person is facing criminal charges. Thus information stored in the smart phones and other gadgets also reflects the mental element of person and therefore compelling a person to give unlock these devices by giving biometric details such as fingerprints should also be brought under the protective clause of right against self-incrimination.

Recently, the Northern District court of California, Judge Westmore ruled that governments have no right to force suspects to unlock devices through biometric features as the fingerprints or face-ids or iris scan cannot be treated as same as physical body evidence. Further Justice Westmore remarked that the biometric features are analogous to 20 physiological, nonverbal responses identified during polygraphy test and thus are considered as testimonial. [21]

> What difference a password, face-id or fingerprints make when the purpose of all is to protect the data and information from third party interference and to conveying our mental taste and preference to intruders. Therefore compelling a person to give bio-metric

[19] 890 N.W.2d 143, 149 (Minn. Ct. App. 2017).
[20] (2010)7SCC263.
[21] Thomas Brewster, Feds Can't Force You to Unlock Your iphone With Finger Or Face, https://www.forbes.com/sites/thomasbrewster/2019/01/14/feds-cant-force-you-to-unlock-your-iphone-with-finger-or-face-judge-rules/#6e057e6642b7 (last visited 27 January 2020).

information to unlock smart devices shall also be read under the article 20(3) of the Constitution.

PART-II

ISSUE OF COMPELLED FINGERPRINTS AND OTHER BIOMETRIC INFORMATION AND THE RIGHT TO PRIVACY

Article 20(3) has one more significant facet which is Right to Privacy. One of the important case from the perspective of privacy jurisprudence was *Kharak Singh v. State of U.P.*[22] where justice Subba Rao in his dissenting judgment held that right to personal liberty under art 21 also extends to be free from any encroachments and intrusions on private life and therefore cannot be remained confined to only as a right to be free from restraints on movements. Right to privacy is an essential ingredient of right to personal liberty under article 21 of the Constitution. Subsequently in *Gobind v State*[23], the Supreme Court for the very first time granted the right to privacy flowing from the person's right to life and personal liberty. It was strongly emphasized that individuals and those traits fundamental to his personality shall be free from the trespass of state authorities. In another landmark case of *Selvi*[24], where the apex court for the first time emphasize on the link between right to fair trial and due process with the right against self incrimination. The apex court also went on to state that right against self incrimination must be treated as one of the important components of right to life and personal liberty and the person has a right to non-interference in the personal autonomy and mental privacy. Finally in *K.S. Puttaswamy*[25], Supreme Court has made it crystal loud and clear that Right to Privacy is the intrinsic part of Right to Life and Liberty under art 21 of the Constitution and urged the Government to create data protection regimes in order to protect and respect the privacy of individuals.

The current environment for testimonial evidence is outdated and is required to be upgraded in modern times. In this era of technological advancements where, biometric data including fingerprints or eye retina are used as a encryption source in mobile and smart devices, then courts should be cautious in applying the doctrine of self-incrimination and testimonial evidence so as to make sure that the intrinsically valuable constitutional right to privacy is not

[22] AIR 1963 SC 1295.

[23] *Gobind v State* (1975) 2 SCC 148 .

[24] Supra note 18.

[25] *K.S. Puttaswamy v. Union of India,* (2017) 10 SCC 1.

being violated and not to give government an uncontrollable access to the most private contents stored in the people's smart devices.

Each person stores and saves certain private information of his mind in his/her mobile phone and other smart devices which are meant to be remain confined and accessible to himself or herself. When the government compels an individual to unlock these mobiles and smart gadgets then it involves risk disclosing those private contents which the person wanted to keep away from the world. When the individual is compelled by the State machineries to disclose the contents of his mind or the contents of his Smartphones by unlocking it even through biometric source then it involves revealing private contents which the individual does not want to share. However if the government obtains the information or access the contents of mobile phones through other means and not by compelling the individual itself then that information would lose its private nature as there would be the secondary or other public means of accessing it. If the information is obtained through such public measures then this necessarily signifies that an individual either implicitly or explicitly made the information public and thus such information lose its private nature.

The scheme of the constitution is such that it allows the interlinkage between right to privacy flowing from the right to life and personal liberty and right against self-incrimination. As it was rightly stated in *Selvi*[26] that person's decision to make a statement is a product of his private choice and there should not be any scope for any invader to interfere with such personal autonomy and especially when the person is facing criminal charges. On account of how society uses smart phones, they have now become the microsm of an individual.[27] State authorities compelling a person to unlock mobile or other smart gadget involves potential risk of disclosing the information about person which may be incriminatory in nature and this state instituted compulsion would be equivalent of violating the right against self incrimination and right to privacy.

POSITION OF LAW IN USA

The views of U.S. Supreme Court on the principle of privacy and right against self incrimination are such that they favor the justification that compelled self-incrimination

[26] Supra note 18.

[27] Efen Lemus, "When Fingerprints Are Key: Reinstating Privacy to the Privilege Against Self-Incrimination in Light of Fingerprint Encryption in Smartphones" 70 *Singapore Management University Law Review* 534-549 (Dedman School of Law 2017).

invades person's privacy. In *Olmteds*[28] case, Justice Brandies in dissent judgment held that "*Fifth Amendment is one of the prime pillars of constitution because it protects the individual and his sanctities of his home and his private life from government invasion*". In *Murphy*[29], Justice Goldberg noted that privacy is one of those noble aspirations that the country's founder aimed to protect through Fifth Amendment. In his view, Fifth Amendment is a shield to protect the innocent from the government's encroachment in his private enclave. Furthermore in *Griswold*[30], Justice Douglas writing for his majority decision held that "*self incrimination clause under Fifth Amendment creates a zone of privacy which no government is allowed to enter into by compelling the individual.*"

Acknowledging the importance of right to privacy, the government should refrain from compelling individuals to surrender their autonomy and control very their personal information. The very premise that individual shall not be compelled to reveal information against himself, shows that right to privacy is implicitly provided under right against self incrimination.[31] Therefore it can be noted that the right against self-incrimination derives its sanctity from the fact that a person's privacy is breached when a third party obtains the sensitive information against the wishes of that person.

CONCLUSION

Right against self incrimination enshrined under art 20(3) of the constitution is regarded as one of the most sacrosanct right. In short right against self-incrimination is a right to remain silent when the accused is face with the incriminating questions. In the digital age, such a constitutional right needs to be extended to such personal smart phones and gadgets as they come to hold more private and sensitive information about a person and thus can serve as a strong source of evidence, ready to be deployed against the person.

As we entered a new digital era; it is imperative on the part of the state to ensure that the fundamental rights as enshrined in the constitution can never be curtailed. In light of technological departure from passwords to biometric data as an alternative tool of decryption, it is necessary that the constitutional protection rights and standards which are being applied

[28] *Olmstead v. United States*, 277 U.S. (1928).
[29] *Murphy v. Waterfront Comm'n of N.Y. Harbor*, 378 U.S. (1964).
[30] *Griswold v Connecticut* 381 U.S. (1965).
[31] Aditya Sarmah," Privacy and the Right Against Self-Incrimination: Theorising a Criminal Process in the Context of Personal Gadgets", 3.2 CALQ (2017) 28.

in case of normal passwords on the gadgets and smart devices must be extend to encompass the biometric passwords as the biometric data form of decryption equally comes under the protection given under the constitution. The smart devices and the information stored in them are the fertile sources of evidence which can be used against the accused. The data stored in them represents the contents of the mind of an individual and thus information stored in those smart devices is just the extension of mind. Therefore compelling the accused to unlock the smart device through biometric password would also amount to giving the testimony and becoming the witness against one self. In today's digital era, there is a strong urgency to extend the protection of right against self-incrimination to the biometric passwords as well.

Similarly the courts should necessarily incorporate the right to privacy into the nucleus of the right against self-incrimination while deciding if the act is testimonial. The gross invasion of privacy from the government machinery by encroaching on the personal data stored in the smart devices shakes the fundamental pillars of the constitution. Thus there is a strong need to effectively expand the doctrine of self-incrimination to cover smart phones and devices.