PRIVACY AND THE RIGHT AGAINST SELF-INCRIMINATION: THEORISING A CRIMINAL PROCESS IN THE CONTEXT OF PERSONAL GADGETS

Aditya Sarmah[*]

ABSTRACT

The right against self-incrimination, enshrined in Article 20(3), is one of the most compelling rights in Part III of the Constitution. Regarded as sacrosanct by the framers of the Constitution, its importance has been exhorted in several judicial decisions across the world. This right is commonly understood to allow the accused to lawfully remain silent when advanced with incriminating questions. However, this generality through which it is usually described has severely limited its scope. Exercising the right to remain silent in the face of an incriminating question is only one facet of the right against self-incrimination. In this article, I seek to highlight how the right against self-incrimination is premised on the right to privacy and further analyse the implications of this interrelationship vis-à-vis one of the most omnipresent objects today: personal gadgets. I argue that the protection under Article 20(3) should be extended to such gadgets; especially as they come to hold more and more information about us in the Digital Age and can serve as an excellent source of evidence, readily available to be deployed against an individual.

INTRODUCTION

Over the last decade or so, the number of Indians who own personal gadgets, and the number of personal gadgets Indians own has increased manifold. Laptops, tablets and smartphones have all become ubiquitous. The number of Indians who use smartphones numbered over 200 million, as of last year.[1] Personal gadgets ensure better connectivity and accessibility for the common man. Various applications available on smartphones and tablets provide for a multitude of services including instant messaging, e-mail, online dating, location mapping and GPS. According to a Morgan Stanley report, the total number of Internet users in India is expected to exceed 600 million by 2020.[2] This kind of accessibility has made the Internet a forum for the dissemination of ideas and thought, a treasure trove of knowledge and has even helped spark

[*] Fourth Year, B.A. LL.B. (Hons.), The West Bengal National University of Juridical Sciences, Kolkata

[1] Leslie 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 June 11, 2016).

[2] *Id.*

social movements and run political campaigns in recent years. What these personal gadgets also represent, however, is a useful insight into the personality and activities of an individual and have emerged as an excellent source of information, which can be used against an individual in a criminal trial.[3] Investigative agencies are empowered to seize various personal gadgets during the course of their investigations.[4] It is in these circumstances that concerns have been raised about the individual's right against self-incrimination and the individual's right to privacy.[5] Both these rights are fundamental rights under the Indian Constitution, the former explicitly provided for under Article 20(3) of the Constitution,[6] while the latter has been read into Article 21 of the Constitution.[7]

This interrelationship between privacy and the right against self-incrimination has not been explored much by the Indian courts, which have been altogether reluctant to engage with either right in a dynamic manner. A few years ago, however the Supreme Court examined Article 20(3) in a detailed manner in *Selvi v. State of Karnataka*,[8] highlighting the interrelationship between Article 21 and Article 20(3), by analysing how privacy and the right against self-incrimination share a fundamentally complementary relationship. The judgment also marked a shift in the nature of the Indian criminal process. It is this relationship and its implications that I seek to explore, while addressing the concerns over using personal gadgets as source of evidence. Under Part II, I shall trace the important case law relating to Article 20(3), and using H.L. Packer's seminal essay, "*Two Models of the Criminal Process*," as a basis, discuss the shift in Indian jurisprudence from the crime control model to the due process model. Thereafter, under Part III, I shall discuss privacy in the Indian context and its complementarity with Article 20(3). Under Part IV, I shall analyse this interplay of privacy and the right against self-incrimination in the context of personal gadgets bearing in mind the jurisprudential gravitation towards the due process model. I shall also attempt to theorise a criminal framework within the Indian constitutional framework. Finally, under Part V, I shall give my concluding thoughts on the subject.

---

[3] *See* Caren Myers Morrison, *Passwords, Profiles, and the Privilege Against Self-Incrimination: Facebook and the Fifth Amendment*, 65 ARK.L.REV. 131, 135-38 (2012). ("Morrison")

[4] §91, CODE CRIM. PROC.. ('CrPC').

[5] Morrison, *supra* note 3, 157-58; Susan W. Brennier, *Encryption , Smart Phones and the Fifth Amendment*, 33 WHITTIER L. REV. 525, 528-30 (2011-2012) ("Brennier").

[6] INDIA CONST. art. 20(3). "No person accused of an offence shall be compelled to be a witness against himself."

[7] INDIA CONST. art. 21. "No person shall be deprived of his life and personal liberty except according to procedure established by law."

[8] (2010) 7 S.C.C. 263 (India) ("Selvi").

II. *SELVI V. STATE OF KARNATAKA* AND THE SHIFT TOWARDS THE DUE PROCESS MODEL

In his seminal work, *Two Models of the Criminal Process*, Packer draws a distinction between the ideologies underlying the two hypothetical models of the criminal process – the Crime Control Model ('CCM') and the Due Process Model ('DPM').[9] The manner in which the criminal process operates in the context of these two models underlies the nature of rights an individual can expect to exercise when faced with the threat of criminal prosecution. As the names of the models themselves suggest, the CCM is aimed at minimizing, and if possible, eliminating crime altogether, while the primary focus of the DPM is on ensuring that the rights of the individuals involved in a criminal trial are not unduly abridged in this quest for eliminating crime.[10] The manner in which the criminal process behaves becomes extremely important in the context of the right against self-incrimination and its privacy rationalisation. Essentially, in a criminal process premised on the CCM, preventing access to an individual's personal information on grounds that it may be incriminating would be antithetical to the ultimate goal of minimising crime, especially when such information can be of immense assistance to investigative agencies. Conversely, the DPM not only recognises the paramountcy of the right against self-incrimination, but would also acknowledge that the unhindered ability of the state to access an individual's personal information is inherently problematic.

Thus, extending the protection of the right against self-incrimination to personal gadgets would only be possible in a criminal process which places a premium on the rights of the individual and does not allow an abridgement of these rights – namely, the DPM. The transition of the Indian criminal process in the context of the right against self-incrimination, from the CCM to the DPM (as marked by the judicial pronouncement in *Selvi*) is therefore crucial in extending the protection guaranteed by Article 20(3) to personal gadgets. I shall first describe in detail both the DPM and the CCM and thereafter trace the abovementioned transition of the Indian criminal process.

A. AN OUTLINE OF THE TWO MODELS OF CRIMINAL PROCESS

[9] Herbert Packer, *Two Models of the Criminal Process*, 113(1) U.PA.L.REV 1 (1964). ('Packer')

[10] The most succinct way to summarise the distinction between the two models is perhaps one of Packer's own analogies wherein he likens the crime control model to a "assembly line or a conveyor belt," which "moves an endless stream of cases...carrying the cases to workers to who stand at fixed stations and who perform on each case as it comes by the same small but essential operation that brings it one step closer to being a finished product," and the due process model to an "obstacle course" where each "of its successive stages is designed to prevent formidable impediments to carrying the accused any further along in the process." *Id.*

In the CCM, the preponderance of crime is looked upon as failure of the law enforcement and justice system, and is said to lead to an utter disregard for the law which ultimately results in a "breakdown of the public order."[11] The CCM therefore focuses on a criminal process that can screen suspects, determine guilt, and secure appropriate dispositions of persons convicted of crime with maximum efficiency. In doing so, the occasional violation of the rights of an individual is justified on the ground that the criminal process functions to guarantee "social freedom," and a failure to do so, would lead to the restriction of the fundamental rights of the individual.[12]

To the contrary, the DPM emphasizes the paramountcy of the rights of the individual, insisting on the elimination of factual and legal errors.[13] It is premised on the belief that the protection of the innocent is far more important than the conviction of the guilty.[14] It also challenges the fundamental premise of the CCM – that the efficiency with which the criminal process deals with a large number of cases is the best indicator of its success.[15] Instead it recognizes that the stigma and the loss of liberty associated with criminal sanction is grave –often exacerbated by the coercive nature of state power and perpetuated by the possibility of abuse and error. In this regard, the DPM considers the trade-off between efficiency and the prevention of oppression of individuals as desirable.[16] Another important value the DPM seeks to uphold is that of equality by imposing upon the government an obligation to provide the accused with adequate protection and minimize the degree to which criminal process may be skewed towards persons in positions of privilege.[17] At its most extreme, it even questions the utility of the criminal sanction.[18]

How do both these models operate *vis-à-vis* each other? For instance, success in the CCM is based on a high percentage of apprehension and conviction as against the rate of crime, and therefore requires minimal delay and minimal challenge to the various steps of prosecution. Conversely, the DPM requires a rigorous analysis along adjudicative lines to remove all

[11] Packer, *supra* note 9 at 9.

[12] *Id*, 10.

[13] *Id*, 15.

[14] *Id,* 15, This notion is also understood as the rationale for the legal maxim, "innocent until proven guilty," *see* Kenneth Pennington, *Innocent until Proven Guilty: The Origins of a Legal Maxim*, 63 THE JURIST 106, 107 (2003).

[15] Packer, *supra* note 9, 15.

[16] *Id*, 16.

[17] *Id.*

[18] *Id*, 20.

possibility of doubt about a given set of facts – a delay to ensure this removal of doubt as such is condoned.[19] An extension of this is the fact that the CCM considers the formal adjudicative process as a "ceremonious ritual,"[20] whereas the DPM regards these "rituals", and its various facets – double jeopardy, the right against self-incrimination, the right to counsel, the notion of criminal responsibility – as integral to the criminal process.[21] An important manifestation of the same is the presumption of guilt in the CCM is juxtaposed with the presumption of innocence in the latter. The presumption of innocence requires procedural conformity, and officials acting within their strictly delineated duties to prosecute an individual, proving the commission of crime beyond all reasonable doubt.[22] The CCM in this regard condones illegal arrests, coercive interrogative methods, illegal evidence and invasive searches, so long as the larger aim of preventing crime is observed – premised on the presumption that the suspect is guilty.[23] It must be noted that a given criminal process in a state operates as a mix of the two models, with the criminal process resembling a production possibility curve with the CCM on one end and the DPM on the other.[24]

B. THE INDIAN CRIMINAL PROCESS WITH SPECIAL EMPHASIS ON THE RIGHT AGAINST SELF-INCRIMINATION

As explained above, the right against self-incrimination is firmly rooted in the DPM, while its position is somewhat suspect in the CCM. Several proponents of the latter model have challenged the very premise of the right. Some have described the right as an anachronism,[25] while others have questioned the validity of the assumptions it makes.[26] However, seeing how the Constitutional framers gave it a sacred position under Part III of the Constitution, and further, seeing how the judiciary has treated the right as sacrosanct[27] (in light of the "third rate

---

[19] *Id*, 10-14.

[20] *Id*, 10-11.

[21] *Id*, 17.

[22] Packer, *supra* note 9, 17.

[23] *Id*, 18.

[24] Jeffery Walker, *A Comparative Discussion on the Privilege against Self Incrimination*, 14 N.Y.L.SCH.J.INT'L & COMP.L. 1,11 (1993) ("Walker")

[25] *See* Ronald Allen, *Theorising about Self Incrimination*, 30(3) CARDOZO.L.REV. 729,731 (2008) ("Allen"); Walker, *supra* note 24, 4-5.

[26] *Id*; David Dolinko, *Is There a Rationale for the Privilege against Self Incrimination?*, 33 UCLA L. REV. 1063 (1985-1986) ("Dolinko").

[27] *See* Nandini Satpathy v. P.L. Dani, AIR 1961 SC 1025 (India); Kartar Singh v. State of Punjab, (1994) 3 SCC 569 (India); D.K.Basu v. State of W.B, (1997) 1 SCC 416 (India).

methods" used by the police), it would be fair to presume that the right against self incrimination has a well-defined value in the Indian context. This is also supported by the fact that along with Article 21, Article 20 is the only other right that cannot stand suspended when an emergency is declared.[28] The linkage between Article 21 and Article 20(3) was also duly acknowledged by the bench in *Selvi*.

Post-independence, the criminal justice system in India tilted towards the CCM[29] and this inclination was also reflected in the interpretation of Article 20(3), as evinced by the landmark judgments of *M.P. Sharma v. Satish Chandra*[30] and *State of Bombay v. Kathi Kalu Oghad*.[31] The former decision upheld the constitutionality of the issuance of search warrants and the seizure of private documents *vis-à-vis* Article 20(3). The majority in the latter decision (an eleven judge bench) upheld the constitutionality of handwriting samples, fingerprints, thumbprints, palm prints, footprints or signatures obtained from the accused. It also held that the giving of a statement by an accused in police custody did not lead to an assumption that the same was a product of coercion.

Far more significant is the philosophy underlying these two decisions. For instance, *M.P. Sharma* held that the power of search and seizure was an *overriding power* of the state for the protection of social security, and could only be regulated by law. Furthermore, it also expressly excluded the right to privacy from the ambit of Article 20(3), stating that importing the right to privacy into a "totally different fundamental right" could not be justified.[32] Perhaps an even more express inclination towards the CCM is the pronouncement that the occasional error committed by the judiciary is not grounds enough to "assume circumvention of the Constitutional guarantee."[33] Such observations were clearly reflective of an attitude which prioritized the suppression of crime, even if it meant the occasional violation of individual rights.

---

[28] INDIA CONST. art. 359.

[29] This is perhaps best captured by Mukherjea J. in A.K. Gopalan v. State of Madras (AIR 1950 SC 27) (India) wherein he emphasized that the enjoyment of various liberties required that the powers of arrest, search, imprisonment and punishment be exercised by the state to ensure that these liberties are protected from "thieves and marauders." Jagmohan Singh v. State of U.P. (AIR 1973 SC 947) (India) is another decision reflective of this attitude, wherein the death penalty was upheld on the grounds that it serves as an effective deterrent mechanism and was indicative of the condemnation of society.

[30] AIR 1954 SC 300 (India) ("M.P. Sharma").

[31] AIR 1961 SC 1808 (India) ("Oghad").

[32] M.P. Sharma, *supra* note 30.

[33] *Id.*

Similarly, *Oghad* limited the scope of self-incrimination to information conveyed only in the personal knowledge of the person providing information and excluding "the mechanical process of producing documents in court…which do[es] not contain any statement of the accused based on his personal knowledge."[34] Further while *Oghad* did place emphasis on the volition on the accused to give personal testimony, it expressly excluded handwriting samples or finger impressions on the ground that the intrinsic character of such evidence could not be changed, and that such evidence produced was only a basis for comparison. In this regard, the Court held that the right against self-incrimination was limited to only such material that by itself had an incriminatory character on the accused – such as a letter confessing to a crime as opposed to a mere handwriting sample. *Oghad* is reflective of the CCM insofar as the method of comparison it upholds is based on a presumption of guilt of the suspect, who if guilty, is to be prosecuted, and if not, is to be acquitted as expeditiously as possible. This manifests itself in the fact that evidence such as blood samples or handwriting samples are beyond the control of the accused and *cannot be manipulated*. Therefore it can be confirmed, as opposed to perhaps, a "statement", which can be distorted to the advantage of the accused[35] and thus retains an element of doubt.

However, both these decisions were rendered before two important developments in Indian jurisprudence – the right to privacy and *Maneka Gandhi*.[36] The latter is responsible for a tectonic shift in Indian jurisprudence, with the judgment considerably widening the ambit of personal liberty under Article 21, to include substantive due process. *Maneka Gandhi* has since played a crucial role, helping the expansion of Article 21, particularly insofar as the rights of the accused are concerned, to include the right to a fair trial, the right to a speedy trial and the right to dignified treatment.[37] The judgment has led to a "humanistic interpretation" of constitutional guarantees, which has emphasized and enlarged the rights of the accused.[38] This rationale played a significant underlying role in *Selvi* where the use of narcoanalysis, the polygraph tests, and brain mapping during the course of investigation was held to be unconstitutional.

---

[34] Oghad, *supra* note 31.

[35] Gautam Bhatia, *Privacy, Self Incrimination and the Constitution – IV: Selvi and the Middle Way*, INDIAN CONSTITUTIONAL LAW AND PHILOSOPHY (June 11, 2016) https://indconlawphil.wordpress.com/2014/09/26/privacy-self-incrimination-and-the-constitution-iv-selvi-and-the-middle-way/.

[36] Maneka Gandhi v. Union of India, (1978) 2 SCR 621 (India) ("Maneka Gandhi").

[37] S.N. Sharma, *Towards a Crime Control Model*, 49(4) JILI 543,48 (2007).

[38] P.N. Bhagwati, *Human Rights in the Criminal Justice System*, 27(1) JILI 1 (1985).

The implications of *Selvi* are enormous for criminal jurisprudence in India. Throughout the judgment, the Court's leaning towards the DPM is evident. In its analysis, the Court linked the right to a fair trial and substantive due process with the right against self-incrimination and made this combined reading of Article 21 and Article 20(3) the bedrock of its entire analysis. The Court went so far as to state that the right against self-incrimination ought to be "read as a component of personal liberty under Article 21,"[39] and then further extended this to include non-interference with the personal autonomy and the mental privacy of the accused as the basis of the right against self-incrimination.

Therefore what sets *Selvi* apart from the catena of judgments which preceded it, is that it recognizes the paramountcy of the rights of the accused and the need to protect citizens from coercive and intrusive (yet not necessarily *physical*) investigative methods. Moreover, *Selvi* is also the first Indian judgment to actually recognize the interrelationship between the right to privacy and Article 20(3). Interestingly, *Selvi* treats this interrelationship as self-evident. Thus it would appear that the onus on the India judiciary henceforth would be to acknowledge (and not necessarily justify) this relationship and develop it further. That being said, it must be borne in mind that *Selvi* does not completely shift the balance in favour of the DPM. Instead a more accurate description of the decision would be the movement along the production possibility curve of the criminal process towards the DPM, and a juncture from which decisions in the future can attempt to further explore the DPM in the Indian context.

III. EXPLORING THE PRIVACY RATIONALISATION OF THE RIGHT AGAINST SELF-INCRIMINATION: THE INTERRELATIONSHIP BETWEEN ARTICLE 20(3) AND PRIVACY IN THE INDIAN CONTEXT

Construing the relationship between the right to privacy and the right against self-incrimination as a harmonious interrelationship – as was done in *Selvi* – has often come in for attack from various scholars.[40] Alex Stein, one of the biggest proponents of the right against self-incrimination has described the 'privacy defense' of the right as flawed.[41] Moreover, the right to privacy is still a nascent right in India, lacks a clear definition, and is prone to a reductionist

[39] Selvi, *supra* note 8, ¶225; For a more in-depth analysis of the link between Article 20 and Article 21, *see* H.M. SEERVAI, CONSTITUTIONAL LAW OF INDIA (VOL. 2), 984 (4th ed., 2014 reprint) ("SEERVAI").

[40] Akhil Amar & Renée Lettow, *Fifth Amendment First Principles: The Self-Incrimination Clause*, 93 MICH. L.REV. 857,890-91 (1995); Dolinko, *supra* note 26, 1107-37; William Stuntz, *Self-Incrimination and Excuse*, 88 COLUM. L. REV. 1227,1234 (1988).

[41] Alex Stein, *The Right to Silence helps the Innocent: A Response to Critics*, 30(3) CARDOZO L.REV. 1115, 1122 (2008).

approach which often prioritizes other interests over the right to privacy.[42] In light of this, is this complementary construction of Article 20(3) and privacy as an accurate one?

I submit that Article 20(3), in fact, should be read in such a manner so as to include within its scope the right to privacy. The most significant development of *Selvi* is that it recognizes that "an individual's decision to make a statement is the *product of a private choice* and there should be *no scope for any other individual to interfere with such autonomy*, especially in circumstances where the person faces exposure to criminal charges or penalties."[43] This pronouncement is an acknowledgment of the interlink between Article 20(3), privacy and personal autonomy. This allows us to utilise the privacy rationalisation of the right against self-incrimination, potentially enabling an expansive reading of Article 20(3). I shall now explain the premise of this privacy rationalisation and thereafter critique the paralysis of the judiciary in developing this interrelationship.

A. THE PRIVACY RATIONALISATION OF THE RIGHT AGAINST SELF-INCRIMINATION: UNDERSTANDING THE "PRIVACY DEFENCE"

The ultimate interest the right to privacy seeks to protect is the "inviolate personality" of the individual,[44] which has been defined as an "individual's independence, dignity and integrity...man's essence as a unique and self-determining being."[45] In relation to this, Ruth Gavison suggests that what the right against self-incrimination protects is the manner in which the information is acquired; and the premise that an *individual ought not to present information against himself*, is a *consequence* of the *right to privacy* the individual possesses.[46] This also answers a common criticism levelled against the privacy defence – if the right against self-incrimination was justified by privacy, then wouldn't third party disclosures anyway defeat its purpose?[47] This is answered by the fact that the right against self-incrimination seeks to protect "the right to a private enclave where the individual may lead a private life"[48] – which in this case is mental privacy. Thus, the individual will not be put in a position where by his *own* actions he would have to abdicate his

[42] Bhairav Acharya, *The Four Parts of Privacy in India*, 50(22) EPW 32, 33 (2015) ("Acharya").

[43] Selvi, *supra* note 8, ¶225.

[44] Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4(5) HARV, L.REV. 193, 205 (1890).

[45] Edward Bloustein, *Privacy as an aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 971 (1964).

[46] Ruth Gavison, *Privacy and the Limits of the Law*, 89(3) YALE L.J. 421, 435 (1980) ("Gavison").

[47] Dolinko, *supra* note 26, 1108.

[48] Miranda v Arizona, 384 US 436, 460 (1966).

autonomous mental processes thereby losing control over the information he wishes to divulge about himself – avoiding what has widely been described as the "*cruel trilemma of perjury, contempt and self accusation*."[49] It has been argued that such divulgence would have adverse effects on the reformative process that most of today's criminal justice systems are premised on.[50]

Redmayne's defence of the right against self-incrimination takes a slightly different approach. He argues that the right against self-incrimination enables the individual to maintain a "distance from the state."[51] This argument implicitly recognises the coercive power of the state, and recognises the possibility of executive overreach. Taslitz further develops this argument by adding that compelled incriminatory statements result in social stigma and mischaracterisation.[52] Minimising this distance between state and citizen would result in an Orwellian dystopia wherein citizens would be subject to immense scrutiny, forcing an individual to act in accordance with the state's "necessitating choice."[53] Therefore Redmayne and Taslitz argue that the right against self-incrimination seeks to preserve the decisional autonomy an individual enjoys – a key component of privacy.[54] A more moderate stance on the above claim would be that rather than remaining inaccessible, individuals are more concerned with personal information being treated in accordance with their expectations.[55] No individual would want that his own disclosures be the reason he is deprived of his personal liberty, or indeed that his own actions compromise his distance from the state.

B. THE REDUCTIONIST NATURE OF THE RIGHT TO PRIVACY IN INDIA.

The above analysis indicates that the right against self-incrimination seeks to protect both information control and decisional autonomy. Courts have recognised that the expression "life and personal liberty" under Article 21 connotes that individuals are entitled to live with dignity.[56] Such an understanding ought to have enabled the maturation of the right to privacy in the Indian

---

[49] Murphy v. Waterfront Comm. of N.Y. Harbor, 378 U.S. 52 (1964); Schmerber v. California, 384 U.S. 757; (1966); R. Kent Greenawalt, *Silence as a Moral and Constitutional Right*, 23 WM. & MARY L. REV. 15, 39 (1981).

[50] Robert Gerstein, *Punishment and Self-Incrimination*, 16 AM. J.JURIS 84, 88 (1971).

[51] Michael Redmayne, *Rethinking the Privilege Against Self-Incrimination*, 27 OXFORD J.LEGAL STUD. 209,225 (2007) as cited in Allen, *supra* note 25, 736.

[52] Andrew E. Taslitz, *Confessing in the Human Voice: A Defense of the Privilege Against Self-Incrimination*, 7 CARDOZO PUB. L. POL'Y & ETHICS J. 121, 136 (2008).

[53] SHANNON BYRD & JOACHIM HRUSCHKA, KANT'S DOCTRINE OF RIGHTS: A COMMENTARY 82 (2008).

[54] *See generally* Gavison, *supra* note 46; Acharya, *supra* note 42, 33.

[55] Helen Nissenbaum, *Privacy as Contextual Integrity*, 79(1) WASHINGTON L.REV. 119,135-151 (2004).

[56] Maneka Gandhi, *supra* note 36.

context, however Indian jurisprudence has remained rather static – largely limiting the scope of the right to privacy to protection against state surveillance.[57]

Kharak Singh v. Union of India[58] was the first Indian case where the Court conceded that a right to privacy exists. The bench, though, made no attempt to reconcile the conflict between the competing interests of privacy and public policy, refusing to read the right to privacy as a part of Article 21. Justice Subba Rao, however, in his noted dissent stated that the right to privacy is "*essential ingredient of personal liberty.*" Subsequently, in *Gobind v. State of M.P.*[59] the Supreme Court, for the first time, granted recognition to the right to privacy as a part of an individual's right to life and personal liberty. It was asserted that the rights and freedoms of citizens set forth in the Constitution guaranteed that the individual, his personality and those characteristics fundamental to his personality should be free from trespass from other individuals and the state. However, the "reductionist approach" towards privacy discussed above, was on full display in *Gobind*, as well as *PUCL v. Union of India*[60] (where the Court declared phone tapping as violative of the right to privacy flowing from personal liberty under Article 21) with the Court subjecting privacy to the "compelling state interest."

Therefore, while the Court did recognise *both* decisional autonomy and information control (fundamental to the privacy-Article 20(3) interlink) as key aspects of privacy in *Selvi*, and arguably even in *Gobind*,[61] courts have failed to move beyond a mere reductionist approach, and in Acharya's words, have failed to construct "a judicial model of privacy that is logical, predictable, and supported by reason."[62] This inchoate understanding of privacy was again on display in *Ram Jethmalani v. Union of India*[63] and *Suresh Koushal v. Naz Foundation*[64] where compelling state interest prevailed over information control and decisional autonomy respectively, with the Court failing to properly delve into either aspect of privacy. This situation will hopefully be rectified by the *Aadhar* case[65] in which the Aadhar card scheme has been challenged as being violative of the

[57] Acharya, *supra* note 42, 35.

[58] AIR 1963 SC 1295 (India).

[59] AIR 1975 SC 1378 (India) ("Gobind").

[60] AIR 1997 SC 568 (India).

[61] Acharya, *supra* note 42, 37.

[62] *Id.*

[63] (2011) 8 SCC 1 (India).

[64] (2014) 1 SCC 1 (India).

[65] K.S. Puttaswamy v. Union of India, Writ Petition (Civil) 494 of 2012 (India).

right to privacy. A three judge bench of the Supreme Court has referred the matter to a larger bench on the basis that there exists a "certain amount of apparent unresolved contradiction in the law declared by this Court."[66] While the government has challenged the very existence of the right to privacy one hopes that the Court does not take such a regressive stance and instead acknowledges its existence while engaging with the right in a far more holistic manner.

Whatever be the outcome of the *Aadhar* case, it is evident the scheme of the Constitution permits an interlinkage between personal liberty, and by extension privacy, with the right against self-incrimination. This recognition of personal liberty under Article 21 as a facet of Article 20(3) cannot be ignored and seems to put to rest the ambiguity which has plagued the debate on the right against self-incrimination in the United States. Resultantly (academic considerations aside), the judicial debate in India needs to focus on the scope of this interrelationship – one willingly accepted by the Supreme Court in *Selvi* – refining it, and providing greater structural clarity, as opposed to having to justify its relationship with the right to privacy. Coupled with the fact that *Selvi* changes the nature of the understanding of the criminal process in India, shifting the emphasis from merely crime control to the rights of the accused, the utility and need for defining this relationship is reinforced. I shall now turn to how personal gadgets fit into this equation and examine whether they ought to be permitted to be used as sources of evidence against an individual.

IV. SELF-INCRIMINATION, PRIVACY AND PERSONAL GADGETS

Having explained the interrelationship between the right to privacy and the right against self-incrimination, I shall now examine the manner in which courts should deal with evidence originating from personal gadgets. In the backdrop of the privacy-Article 20(3) link, the argument I seek to advance is that in using personal data originating from personal gadgets as evidence against an individual compels him to act as a witness against himself, therefore violating the fundamental nature of Article 20(3), as interpreted in *Selvi*. I shall first briefly lay out the legal framework which empowers the state to utilise personal gadgets as a source of information and then highlight the problems with the same. Thereafter, I shall argue how using personal gadgets as a source of evidence against an individual is violative of Article 20(3), anchoring the analysis on its constitutive elements.

A. PRIVACY CONCERNS IN USING PERSONAL GADGETS AS EVIDENCE

[66] *Id*, ¶12.

The state, while carrying out investigations, has a wide power of search and seizure which extends to the seizure of mobiles, personal laptops and other such gadgets as evinced from the provisions of the CrPC.[67] Further, the Information Technology Act empowers the government to intercept personal information for the purposes of investigation of an offence.[68] Thus, investigators have access to a tremendous amount of personal data about an individual, which can be used against him at the stage of investigation and trial.[69] This can range from text messages or other such conversations and call logs to internet history to online personas adopted by the individual. These fertile sources of information offer valuable insight into the character of the individual and can also provide "clinching" evidence.[70] This cluster of provisions relating to search and seizure place a large amount of discretionary power in the hands of police officers, and have minimal safeguards, limited to the recording of reasons, the presence of witnesses or the person while carrying out the search and the preparation of a list of all seized items.[71] Furthermore, in terms of the legal framework for submission of evidence, it is important to note that, unlike the United States, the doctrine of the "fruit of the poisoned tree" is not applicable in India.[72] Therefore, any evidence collected in non-compliance of the abovementioned provisions, or the CrPC in general, is not automatically disqualified from being presented.[73]

It is clear that legislators have focused on a paradigm where efficiency is placed at a premium, without creating a safety net for the possible violation of rights, specifically, the right to privacy. However, in light of the gravitation towards the DPM, as seen in *Selvi*, I shall now explain how

---

[67] §91, CrPC.

[68] §69, The Information Technology Act, 2000 read with the Interception Rules, 2009. For a more thorough understanding of the government's powers under the Information Technology Act, 2000, *see* Prashant Iyengar, *Privacy and the Information Technology Act — Do we have the Safeguards for Electronic Privacy?*, THE CENTRE FOR INTERNET & SOCIETY, April 7, 2011 *available at* http://cis-india.org/internet-governance/blog/privacy/safeguards-for-electronic-privacy (last visited January 19, 2017).

[69] *Id. See* §69B, The Information Technology Act, 2000 which empowers the government to monitor and collect traffic data or information through any computer resource for cyber security; *See generally Internet Privacy in India,* THE CENTRE FOR INTERNET & SOCIETY, *available at* http://cis-india.org/telecom/knowledge-repository-on-internet-access/internet-privacy-in-india (last visited January 19, 2017).

[70] Adam Gershowitz, *The iPhone meets the Fourth Amendment*, 56 UCLA L. REV. 27, 40-45 (2008-2009); Morrison, *supra* note 3, 135-36.

[71] Divij Joshi, *Search and Seizure and the Right to Privacy in the Digital Age: A Comparison of US and India*, THE CENTRE FOR INTERNET AND SOCIETY (June 12, 2016), http://cis-india.org/internet-governance/blog/search-and-seizure-and-right-to-privacy-in-digital-age.

[72] Pooran Mal v. Director of Inspection (Investigation), (1974) 1 SCC 345 (India).

[73] Shyni Varghese v. State (Govt. of NCT of Delhi), (2008) 147 DLT 691 (Del) (India); M.P. Sharma v. Satish Chandra, AIR 1954 SC 300 (India); State of M.P. v. Ramesh C. Sharma, (2005) 12 SCC 628 (India); R.M. Malkani v. State of Maharashtra, (1973) 1 SCC 471 (India); State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600 (India).

the current framework is problematic in the context of personal gadgets, and allowing the police access to the same violates the right against self-incrimination.

Personal information collected from gadgets

The numerous uses of personal gadgets – storing photographs, videos and documents, along with various applications which store personal information – provide an insight into the finances, social and professional life and the physical whereabouts of an individual. Thus, they can produce a significant amount of evidence about an individual.[74] In light of this fact, the current Indian model seems increasingly problematic. Using the information available on an individual's person gadget *against him without consent* violates the sanctity of the private enclave an individual is entitled to, and results in self-incrimination.

Using text messaging conversations, physical locations, social preferences and the myriad of information that can be gleaned from personal gadgets, against an individual is, in essence compelling the accused to serve as a witness against himself *through his own agency*. Essentially this information, made available by compelled seizure of the gadget, is a reflection of the user's thoughts. For instance, a text conversation between two people is an extremely private conversation in which both individuals are essentially expressing thoughts in the form of text communication – these statements being the product of a *private and autonomous* choice – a choice *Selvi* recognizes as *fundamentally sacrosanct and inviolable*, especially under the threat of criminal prosecution.[75] Similarly the use of various applications such as those related to online shopping or finance also reflect the psychological processes of an individual.[76] Another example reflective of the mental processes of an individual would be the browsing history of an individual on the internet or the kind of media he has stored on his computer.[77] Any uninvited or unauthorized third party accessing this information would be a violation of his privacy. Arguably, some of this data, singularly considered, may not in itself be incriminating. However, the sum of this data put together can provide incriminating evidence against an individual.[78]

---

[74] Ber-An Pan, *The Evolving Fourth Amendment: United States v. Jones, The Information Cloud and the Right to Exclude*, 72 MD. L. REV. 997, 1024 (2013).

[75] Selvi, *supra* note 8, ¶225.

[76] *See generally* Michael Bosnjak, Mirta Galesic & Tracy Tuten, *Personality Determinants of online shopping: Explaining online purchase intentions using a hierarchical approach*, 60 JRNL. OF BUSINESS RESEARCH 597 (2007).

[77] *See generally* James McElroy et al., *Dispositional Factors in Internet Use: Personality versus Cognitive Style*, 31(4) MIS QUARTERLY 809 (2007); Richard Landers & John Lounsbury, *An investigation of Big Five and narrow personality traits in relation to Internet usage*, 22 COMPUTERS IN HUMAN BEHAVIOUR 283 (2006).

[78] *See generally* Morrison, *supra* note 3; Brennier, *supra* note 5.

Therefore, using this information against an individual would undermine the amount of information control he can exercise about himself. As explained by Gavison, the right against self-incrimination seeks to protect *this* very breach of privacy.[79] The utilization of the history of an accused on a dating site, or his location as depicted on GPS, or his private communications via e-mail or various messenger services, as evidence against him in a trial would amount to putting him in a position whereby he loses control over the information he wishes to divulge about himself. As elaborated above, this loss of control over one's information is what the right to privacy seeks to protect. And further, because *Selvi* recognises that information control is a *fundamental* aspect to the right against self-incrimination[80] (while couching the interpretation of Article 20(3) in a model akin to the DPM) the use of such information as evidence against an individual certainly does not sit comfortably with the spirit of Article 20(3).

Communications via social media

Communications via social media, which often occur through personal gadgets, also help investigators glean information about individuals and are being increasingly used.[81] However social media presents an interesting conundrum. A number of communications via social media are in fact available in the public domain, and while signing up on such medium, individuals consent to the same being made public.[82] Therefore, a quick Google search of an individual may lead to his Facebook page or his Twitter account. That being said, the amount of access a stranger has to such social media pages can be restricted by the individual himself, from the various privacy options available on such media. Therefore the argument here shall be restricted to situations where an individual is compelled to give investigators access to social media communications which are not public, or to which access has intentionally been restricted. Personal gadgets provide the perfect source for accessing such data.

An individual who frequently participates on social media, unknowingly or knowingly, reveals a number of personality traits. Tweets, Facebook status updates, posts on Reddit and other habitual social media actions collectively reveal a great deal of information about individuals –

[79] Gavison, *supra* note 46, 435.

[80] Selvi, *supra* note 8, ¶¶225-26.

[81] *See* Central Bureau of Investigation, November 2013, *Social Media & Law Enforcement: Challenges and Opportunities*; *SEBI cites 'mutual friends on Facebook' as insider trading evidence*, LIVEMINT, Feb. 7, 2016 *available at* http://www.livemint.com/Money/yAwcckxlrgW3nFh9PEKaDI/Sebi-cites-mutual-friends-on-Facebook-as-evidence-in-insid.html (last visited June 11, 2016).

[82] *See*, *e.g.*, FACEBOOK DATA POLICY, https://www.facebook.com/policy.php (last visited June 12, 2016); TWITTER PRIVACY POLICY, https://twitter.com/privacy?lang=en (last visited June 12, 2016).

their thinking patterns, lifestyles, socio-economic status, philosophical, religious and cultural outlooks.[83] Allowing such evidence to be used against an individual is problematic on two levels. First, the use of such information as evidence undermines the amount of information control an individual has *vis-à-vis* himself, and his expectations as to how information divulged is to be treated. Similar to the problems described above, the use of such information as evidence is a breach of the autonomous mental processes of an individual, and infringes upon his privacy.

The second problem associated with the same is a trisection of the individual's right to privacy, the right against self-incrimination and his right to free speech. The use of such evidence against an individual being prosecuted for having 'liked', 'shared' or commented on an article criticizing a politician, or 'tweeting' something which may be deemed anti-national or anti-secular, or against the moral sentiments of society,[84] forces the individual to act in accordance with the "necessitating choice" of the state. This resultantly leads to a minimization of the distance between him and the state. Therefore, he would constantly have to maintain a persona in compliance with the expectations of the state, and have to ensure that his actions on social media are not potentially incriminatory – leading to a "chilling effect,"[85] on free speech and undermining his autonomy.[86] As discussed above, Redmayne and Taslitz respectively argue that the right against self-incrimination seeks to prevent the erosion of this distance from the state, in addition to preventing mischaracterization. Therefore, the use of social media communications as evidence against an individual would not only undermine the amount of control he has over his own personal information, but would also *violate his decisional autonomy* – a key facet of privacy. Again, with the jurisprudential development of the right against self-incrimination in India and

---

[83] *See generally* Ken Strutin, *Social Media and the Vanishing Points of Ethical and Constitutional Boundaries*, 31(1) PACE L. REV. 228 (2013); Heather Kelly, *Police embrace social media as crime-fighting tool*, CNN, Aug. 30, 2012, http://edition.cnn.com/2012/08/30/tech/social-media/fighting-crime-social-media/ (last visited June 12, 2016).

[84] *See, e.g.*, Kukil Bora, *Arrest For Facebook 'Like' In India Creates Controversy; Is It An Onslaught On Internet Speech?* INTERNATIONAL BUSINESS TIMES, 20 Nov., 2012, available at http://www.ibtimes.com/arrest-facebook-india-creates-controversy-it-onslaught-internet-speech-891142 (last visited June 12, 2016); Prajakta Hebbar, *Two Muslim Men Arrested For Sharing Offensive Photos Of Goddess Kali On Facebook,* The HUFFINGTON POST, May 28, 2016, available at http://www.huffingtonpost.in/2016/05/28/arrested-for-insulting-kali-fb_n_10176306.html (last visited June 12, 2016); Prasanto K Roy, *Why was an Indian man held for sending a tweet*, BBC NEWS, Nov 6, 2012, http://www.bbc.com/news/world-asia-india-20202275 (last visited June 12, 2016; *Thai man arrested for Facebook 'like' of doctored royal photo*, THE GUARDIAN, Dec. 10, 2015, available at https://www.theguardian.com/world/2015/dec/10/thai-man-arrested-facebook-like-photo-king (last visited June 12, 2016.

[85] For a more in-depth discussion on the "chilling effect" of free speech, *see* Shreya Singhal v. Union of India, (2015) 5 SCC 1, ¶¶ 87-94 (India).

[86] To understand the link between autonomy and free speech, *see generally* Susan Brison, *The Autonomy Defence of Free Speech*, 108(2) ETHICS 312-39 (1998); C. Edwin Baker, *Autonomy and Free Speech*, 27 Const. Comment. 251-82 (2010).

civil society becoming increasingly active on social media, an examination of Article 20(3) along the above lines does merit a relook.

B. THEORISING A CRIMINAL PROCESS WITHIN THE CONSTITUTIONAL FRAMEWORK

The concerns highlighted above, both in terms of personal data available on personal gadgets and private (or restricted) communications via social media, were also reflected by the bench in *Selvi* albeit in the context of the various narco-analytic methods discussed. These narco-analytic investigative methods were ultimately deemed unconstitutional, *inter alia*, because of the fact they were violative of the autonomous mental processes of an individual. In light of this, and the larger philosophy prevalent in the judgment indicating a movement of the Indian criminal process towards the DPM, it is certainly intriguing as to how courts will treat evidence gathered from personal gadgets. I shall now with specific reference to Article 20(3), attempt to reconcile the above concerns within the Constitutional framework.

It must be reiterated at this point that for a more holistic development of the right against self-incrimination, privacy jurisprudence in India will require to take a quantum leap. Concepts such as decisional autonomy and information control, fundamental to the right to privacy, still need to be explored by courts in far greater detail. Moreover, courts have to be willing to engage with these concepts at a far greater level of nuance, and not consistently subject the right to privacy to the reductionist approach they have been guilty of doing. Until the jurisprudential understanding of the right to privacy in India coalesces into a more comprehensive one, our understanding of the right against self-incrimination, and its development, shall remain largely stunted.

Assuming, however, that privacy jurisprudence in India does mature, how would it operate in the context of personal gadgets *vis-à-vis* Article 20(3)? According to a Report of the Law Commission of India in 2002,[87] Article 20(3) is regarded as having three aspects – the right of the accused to remain silent and to not incriminate himself, the presumption of innocence of the accused and the imposition of the burden of proving the guilt of the accused beyond all reasonable doubt upon the state.[88] This is particularly interesting, as these facets are all characteristic features of the DPM, and thereby the Law Commission seems to be endorsing the fact that Article 20(3) is to be construed in terms of an interpretation which strongly favours the supremacy of the rights of the individual. It should also be noted that this report was submitted

[87] Law Commission of India, May 2002, *144th Report on Article 20(3) of the Constitution of India and the Right to Silence*.

[88] *Id*, 5.

almost a decade prior to the decision in *Selvi*, which was the most pronounced statement of the judiciary in terms of the shift towards the DPM.

The Law Commission Report is also notable because it reaffirms the importance of Article 20(3) at a time when the right against self-incrimination had been whittled down in the United Kingdom by the Criminal Justice and Public Order Act, 1994 passed by the English Parliament, as well as the Evidence (Northern Ireland) Order, 1988.[89] These legislations allowed an adverse inference to be drawn against the accused when he chose to exercise his right to remain silent. In a ringing endorsement of the right against self-incrimination, the Law Commission highlighted the importance of maintaining the sanctity of the right as enshrined in Article 20(3).[90] It further observed that in light of the developments in *Maneka Gandhi*, whittling down the protection guaranteed by Article 20(3) (even to the extent of drawing an adverse inference from silence) would be unconstitutional.[91] However, while the Law Commission Report was much ahead of Indian jurisprudence at that point, it unfortunately failed to discuss the interrelationship between privacy and the right against self-incrimination – despite comparing Indian jurisprudence of the right against self-incrimination to the United States, where this interrelationship has received far more attention.

As analysed above however, the Indian Constitution seems supportive of a framework which imports the right to privacy in Article 20(3). How would this framework function in the context of personal gadgets? An examination of the wording of Article 20(3) reveals that to avail the right, an individual has to establish three elements: *first,* that he is a person *accused* of an offence; *second* that he was *compelled* to be a witness against himself; and *third* that the incriminatory evidence is *self directed*, that is, against himself. The precise scope of these three components has often generated much debate. I shall now try and explore these controversies, and how they ought to play out in the privacy-right against self-incrimination paradigm, in the context of personal gadgets.

'Accused of an offence'

The right enshrined in Article 20(3) has been understood to extend to an individual against whom criminal proceedings have been initiated; it does not merely extend to court proceedings.[92]

[89] *Id,* 1.

[90] See *supra* note 87 at 2, 45-47.

[91] *Id*, 2, 6, 40.

[92] M.P. Sharma, *supra* note 30; Oghad, *supra* note 31; Selvi *surpa* note 8, ¶125.

However, this protection only extends to cases where a "formal accusation" has been made, which entails an FIR being filed against the concerned individual.[93] As has been observed, this interpretation apparently excludes those classes of cases wherein incriminatory statements can be made prior to an FIR being filed.[94] Examples of this include the powers of the Revenue under Chapter XXII of the Income Tax Act, 1961 or Section 67 read with Sections 42 of the Narcotics Drugs and Psychotropic Substances Act, 1985 ('NDPS'), or Section 11C of the Securities and Exchanges Board of India Act, 1999 (which explicitly provides that such statements may be used against the individual). This interpretation has also been endorsed by courts, distinguishing this pre-investigation stage as an "enquiry phase."[95]

Using the same rationale as above, deploying information against an individual procured from his personal gadget, prior to a formal accusation being made against him, is equally violative over his control of personal information and his decisional autonomy. Merely because an FIR is not yet filed against him does not provide the state with the requisite authority or legitimacy to interfere with his privacy. Therefore a framework, which recognizes the interrelationship between privacy and the right against self-incrimination, will also have to reconcile itself with a probable expansion of the scope of the "accused" under Article 20(3). Thus, an income tax officer going through one's finances as displayed on a financial management application or an officer empowered under the NDPS perusing conversations and search history relating to narcotic substances is still incriminatory even if no FIR (i.e. formal prosecution) has commenced against said individual. Thus such information ought to be covered under the protection under Article 20(3).

'Compelled to be a witness'

The second element of "compulsion" has judicially been interpreted to extend the protection of Article 20(3) to such evidence or statements as is not voluntarily procured.[96] In the context of information accessible solely through personal gadgets, this element of compulsion is relatively easy to ascertain. Any evidence obtained by forcible seizure of the gadget or unauthorized access to purely personal data (information about one's personal life, financial records, location etc.)

[93] Thomas Dana v. State of Punjab, AIR 1959 SC 375; Selvi *surpa* note 8, ¶125.

[94] Abhinav Sekhri, *The Right against Self-Incrimination and its Discontents,* INDIAN CONSTITUTIONAL LAW AND PHILOSOPHY (June 11, 2016) https://indconlawphil.wordpress.com/category/criminal-law-and-the-constitution/article-203/.

[95] Directorate of Enforcement v. Deepak Mahajan, AIR 1994 SC 1775 (India); Romesh Chandra Mehta v. State of West Bengal, AIR 1970 SC 940 (India); Raja Narayanlal Bansilal v. Maneck Phiroz Mistry, AIR 1961 SC 29 (India).

[96] Oghad, *surpa* note 31.

through hacking or other legitimate means, ought to allow the accused to invoke the protection under Article 20(3).

However, this question becomes slightly more ambiguous in the context of social media communications. A number of social media communications, are in fact, publicly accessible. For instance, a third party can view an individual's friends on Facebook or 'connections' on LinkedIn, or browse through select photographs, or view their 'tweets.' In a recent and rather bizarre turn of events, it was reported that criminals in Punjab were publicly proclaiming their criminal activities on social media.[97] Investigators have acknowledged that such communications are a minefield of evidence, and actively use this in prosecutions.[98] Is the procurement of such evidence *compulsion*? A subtle distinction will have to be drawn here. In the case, of *private* communications – such information that cannot reasonably be accessed unless the investigator (or any third party) is specifically allowed to do so – the protection under Article 20(3) must certainly apply.

However, in the case of publicly available photographs or professional connections or status updates, which *can* be accessed without special permission granted by the user of the account, I believe the protection cannot be allowed. While it can be argued that an individual's autonomous processes are still being undermined or that he is being forced to comply with certain choices being imposed upon him by the state, the privacy rationalization of the right against self-incrimination is insufficient here. Simply because the moment any information is made accessible to the public at large, such information is not limited to the individual's "private enclave." This *public* disclosure is made out of his own volition. Therefore, if an individual were to post a 'status update' of him having robbed a casino with pictures of the same, and this were made available to the public at large, the privacy rationalization of Article 20(3) would be insufficient to invoke the right guaranteed under it. An investigator coming across the same would be the equivalent of him hearing the offender in a public space, like a bar or a *maidan*. While standard evidentiary rules still ought to apply to such information I believe, however, that Article 20(3) cannot be invoked in such situations.

'Witness Against Himself'

[97] Indrani Basu, *In Punjab's Nabha Jail, Gangsters Fight On Social Media Over Who Killed 'Rocky', Post Selfies*, THE HUFFINGTON POST, May 2, 2016 *available at* http://www.huffingtonpost.in/2016/05/02/punjab-gangsters-nabha-ja_n_9819568.html (last visited June 11, 2016); Gurvinder Kaur, *Rocky & Gang, this time in Punab*, TEHELKA, MAY 16, 2016 *available at* http://www.tehelka.com/2016/05/rocky-gang-this-time-in-punjab/ (last visited June 11, 2016).

[98] *See* Edward M. Marisco, Jr., *Social Networking Website: Are MySpace and Facebook the fingerprints of the Twenty First Century?*, 19 WIDENER L.J. 967 (2009-2010).

A witness was defined as one who "furnishes evidence" in *M.P. Sharma* and thus any individual who furnishes evidence by way of a "positive volitional act"[99] would have been covered by the scope of Article 20(3). However, the majority in *Oghad* disagreed with this understanding as being too broad, and severely limited it, basing its understanding on principles of common law and other legislation like the Evidence Act, 1872 and the Identification of Prisoners Act, 1920.[100] This understanding in *Oghad* has been criticised as being legally fallacious, subjecting the constitutional intent to colonial era legislations and principles of common law, when it really ought to be the other way around.[101] Such an understanding was also premised heavily on understanding the India criminal process as being based solely on the CCM.[102] It should be noted however that concurring opinion of Justices Das, Sarkar and Das Gupta disagreed with the majority on this point and agreed with the holding of *M.P. Sharma*. However they premised their analysis in terms of the CCM,[103] and in light of *Selvi*, their holding is of limited relevance to the argument proposed in this essay.

Oghad then went on to define a witness as one who "imparts knowledge in respect of relevant fact, by means of oral statements or statements in writing, by a person who has personal knowledge of the facts to be communicated to a court or to a person holding an enquiry or investigation."[104] The understanding in *Oghad* was that if the relevant information was in itself capable of incriminating the accused, only then should the protection under Article 20(3) be allowed. In *Oghad*, it was held that since fingerprints, blood samples or handwriting samples were not in themselves incriminating, the accused would not be allowed to invoke Article 20(3).

Now, certain information (of the type which is incriminatory *per se*) available on personal gadgets and social media communications should fall within this definition as postulated by *Oghad*. While the judgment in *Oghad* was delivered much before the idea of personal gadgets had properly even been conceived, it is unlikely that the definition would exclude such information. After all, it is in itself capable of incriminating the accused. However, it may also be possible that while information might not *in itself* be incriminatory, it may be lead to adverse inferences being drawn

[99] M.P. Sharma, *supra* note 30.

[100] Oghad, *surpa* note 31.

[101] Gautam Bhatia, *Privacy, Self Incrimination and Article 20(3) – II: Kathi Kalu Oghad*, INDIAN CONSTITUTIONAL LAW AND PHILOSOPHY (June 11, 2016) https://indconlawphil.wordpress.com/category/criminal-law-and-the-constitution/article-203/.

[102] *Id.*

[103] *Id.*

[104] Oghad, *supra* note 31.

against the individual. Music or video preferences or one's browsing history on the Internet or indeed sharing, retweeting or liking certain articles or tweets may be construed as evidence to be used as against an individual. Thus, the fact that there might be music present on an individual's cell phone which may be described as misogynistic or that he may be a frequent viewer of pornographic content ought not to lead to any adverse inferences in a trial for sexual assault or rape. Likewise, the sharing or liking of an article or tweeting, supporting or criticizing certain political ideology ought not to be used as evidence against an individual (subject to the same only being visible to those who are 'friends' or any such limitation being placed on the same). Such tastes and preferences are the consequence of mental autonomous preferences, and as stated in *Selvi*, there ought to be "no scope for any other individual to interfere with such autonomy…especially in circumstances where people face exposure to criminal charges or penalty."[105]

Thus, in terms of rationalizing Article 20(3) in terms of the right to privacy, the understanding of "to be a witness against himself" would ideally have to be expanded and refined – probably reverting to the meaning of the phrase as understood by *M.P Sharma.*

Thus developing the interrelationship between Article 20(3) and the right to privacy, in the context of personal gadgets, in a holistic manner will require considerable alterations in the treatment of the right. Certain specific questions will have to be answered in due course as well. For example, what about those instances (such as cyberbullying or cyberstalking) where the primary source of evidence will be available only through personal gadgets? In my opinion, in such instances, where the primary evidence collected via personal gadgets is absolutely indispensible, then, the legislature ought to specifically legislate on the same. In the absence of any legislation, there must be a burden on the prosecution (a considerably high one at that) to show that such evidence is absolutely necessary for the case at hand, and that prosecution or investigation cannot proceed without the same. Furthermore, the same should only be allowed in very specific situations.

Further, even if evidence obtained from personal gadgets and social media communications is presented at a trial, the same should be deemed altogether irrelevant. Ideally, under the doctrine of the fruit of the poisoned tree such evidence would not be admitted in the first place,[106] however, as discussed above, Indian jurisprudence doesn't recognize the same. Thus, the judge

[105] Selvi, *supra* note 8, ¶225.

[106] For a justification of the doctrine within the framework of the Indian Constitution, *see* SEERVAI, *supra* note 39, 1075-76.

ought to consider such evidence irrelevant to the present proceedings. This is far from a foolproof scenario, and certainly not desirable. Judges are human as well, and even under the best intentions, might construe information obtained from personal gadgets as being incriminatory, especially if deployed skillfully by the prosecution. Thus it would be far better if such evidence would not be admitted in the first place at all, and any mention of the same, redacted. What definitely must be disallowed is the questioning of the accused pertaining to such evidence. Several other such questions will gradually arise relating to a criminal process which premises its right against self-incrimination on a due process model, which the judiciary will have to deal with in a proactive manner, ensuring that the rights of the accused are given paramountcy.

V. CONCLUSION

These are certainly interesting times for criminal jurisprudence in India, with *Selvi* representing one such watershed moment. The transition from a model based solely on the CCM, to one which acknowledges and realises the paramountcy of the rights of the accused, specifically in the context of the right against self-incrimination will have resounding consequences. It is significant, in itself, that *Selvi* recognises this interlink between the right against self-incrimination (enshrined in Article 20(3) of the Constitution) and the right to privacy which has been read into Article 21 of the Constitution. However at the cost of repetition, for a holistic development of this interrelationship, the Indian judiciary will have to address privacy in a far more dynamic manner, and ensure that it abandons the reductionist approach it is guilty of employing far too often.

What is also important to note, however, is that the constitutional scheme provides sufficient basis for the development of this interrelationship. This is precisely what enables Indian jurisprudence to move beyond the criticism levelled against the privacy rationalisation in other common law jurisdictions. Using the theories postulated by various scholars who support this interrelationship is therefore far more readily acceptable in India. Of course, this entire development is premised on the understanding that the Indian criminal process is heading towards one based on the DPM – a claim which needs to explored in a greater detail to truly crystallise.

It is in this backdrop that the question of personal gadgets becomes so much more precarious. These gadgets represent a fertile source of evidence which can be utilised against the accused by investigators to great success (and possibly damage as well). However, if the understanding of

the privacy-right against self-incrimination interrelationship is correct then such use must not be allowed. Aside from problems with reliability, such use represents gross invasions of privacy by the state machinery – both in terms of personal data stored on gadgets and social media communications of a personal nature – as highlighted above. To effectively expand the scope of the right against self-incrimination to cover personal gadgets, however, certain important changes will have to take place in the way the courts have understood the three facets of Article 20(3). On a more philosophical note, the Extended Mind Hypothesis, in fact, even regards personal gadgets as an extension of the mind.[107] While of course not applicable to legal proceedings, from a strictly moral point of view, this seems to bolster the argument for extending Article 20(3) to personal gadgets.

I do concede that the development of Article 20(3) to effectively cover personal gadgets will be far from straightforward. However, I strongly believe that the constitutional scheme encourages the rationalisation of Article 20(3) in terms of the right to privacy. Only if this interrelationship is allowed to coalesce, will Article 20(3) effectively cover personal gadgets. Exceptions may still need to be created. However, the same must be created only in extremely specific circumstances and difficult to invoke. The important first step for the courts, in this regard, would be to develop privacy jurisprudence in India. Only then can the understanding of the importance of data made available through personal gadgets, as self-incriminatory be allowed to crystallise, thereby allowing the accused to invoke Article 20(3). Once the courts are able to achieve this, subsequently the focus ought to be on providing the same with a greater degree of sophistication and nuance, refining the criminal process, and where necessary, carving out exceptions as required.

[107] David Chalmers, *TedxSydney – Is your phone a part of your mind?*, YOUTUBE (June 10, 2016), https://www.youtube.com/watch?v=ksasPjrYFTg (David Chalmers, along with Andy Clark was one of the original proponents of the Extended Mind Hypothesis: *See* Andy Clark & David Chalmers, *The Extended Mind*, 58 ANALYSIS 7 (1998).