Unearthing the Elements of Privacy from the Information and Technology Act, 2000: Data Protection in India

[1*]Sanjana Kulkarni

"The right to privacy is inextricably bound up with all exercises of human liberty – both as it is specifically enumerated across Part III, and as it is guaranteed in the residue under Article 21. It is distributed across the various articles in Part III and, mutatis mutandis, takes the form of whichever of their enjoyment its violation curtails." [2]

Right to privacy is no more a myth - the Supreme Court quite recently conferred this right upon the citizens of India and has deemed it to be a Fundamental Right under Chapter III of the Indian Constitution. Overruling the verdicts given in *M.P. Sharma*[3] and *Kharak Singh*[4], this 547 pages judgement divulges it as a Fundamental Right [5]under the purview of Article 21 and Article 19 of the Constitution respectively. The same has been illuminated with respect to Article 12 of the Universal Declaration of Human Rights which declares:

"*No person shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to protection of the law against such interference.*"[6] , thereby concluding that:

"*Informational Privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but from non-state actors aswell. We commend the Union Government the need to examine and put in place a robust regime for data protection. The creation of such a regime requires a careful and sensitive balance between individual interests and legitimate concerns of the State. The legitimate aims of the State would include for instance protecting national security, preventing and investigating crime, encouraging invasion and the spread of knowledge, and preventing the dissipation of social welfare benefits. These are the matters of policy which are to be considered by the Union Government while designing a carefully structured regime for the protection of data*" [7]

And even though a unified structured statute remains absent, the Government[8], considering the anomalous escalation in the masses availing the facility of Internet, in the year 2000, inaugurated the Information of Technology Act, 2000 which resolves to avert the abuse of and over the internet[9], besides safeguarding the rights and data of the citizens[10]; attempting to make cyber space a safe haven for them. the Act has sundry indiscernible facets of privacy which sustain the fortification of their privacy[11] in a fascinating way- unrevealed below.

In search for the Elements of Privacy in [12]the Act:

> *"Privacy is not an option and should not be the price we accept for just getting on the internet"*
>
> - *Gary Kovacs*[13]

The expression privacy is stipulated as "*the right of a person to be free from intrusion into or publicity concerning matters of a personal nature*"[14], perused by The Constitution of India with respect to its celebrated Article 19[15] and the Article 21[16]. Therefore, the Act catalogues disparate clauses, obtruding austere punishments upon the transgression of these rights[17] in the virtual world. True to its word, the Act thrusts imprisonment or fine[18] upon those who had legal ingress to electronic record, book, register, correspondence, information, document or other material, but divulged the same, without

the consent of the data's keeper[19]. Similarly accessing[20] or abetting *aliquis* access[21] one's computer, its source or network without licit approval of the owner is a crime under this Act, which inadvertently ventures to halt the invasion of privacy in the intangible domain. Along the same lines, it is an offence[22] to infix a virus[23] into the computer and thereby damage[24] the hardware or the software or disrupt[25] the same as it is invasive of his or her "technological space"- thus, privacy. The abstract of Hacking[26], which concerns schlentering unauthorised access to one's computer source or network and then obliterate or tailor the information within[27] is undeniably infiltrative of privacy and *in parallelos*, the Act castigates the same by strictly penalising the hackers. *Etiam*, dissimulating to be a legitimate entity and deceiving the other to glean data over the computational arena is a grave offence under the Act[28], therewithal being violative of their privacy. Identically, this article interprets Section 66d of the Act to be capable of safeguarding one's informational privacy against impersonation and hence, cheating. This has been averred in *National Association of Software and Service Companies V. Ajay Sood*[29], wherein the defendant attempted to use the plaintiff's name for acquiring information from third parties, which was inconceivable under quotidian circumstances. This draws attention to the privacy of the third parties being breached by the defendant, only to be disregarded in the case *de quibus supra*. Similarly, unwarranted entry into the protected system of the Legal Advisor[30] has been condemned by Madras High Court[31]. R*espectu* above utterance, a shielded apparatus is a computer source accessible only to the government; by designated personals on its behalf[32], thus, securing Government's privacy[33]. To reap admittance in the aforesaid "protected system", wherein, exercising its pervert use might stimulate disarray in the State is an act of terrorism[34], according to the Information and Technology Act, 2000[35] and the "terrorist" is subject to imprisonment upto lifetime[36]. In the same context, identity theft, which is practicable only by plundering one's privacy, is declared a serious breach of the Act[37]. Simultaneously, this Act explicitly emphasises upon corporeal seclusion and the stunt of capturing a picture of the bodily part of the mortal without his or her acquiescence is held violative of their respective privacy and is subject to incarceration up to 3 years or a mulct not exceeding Rupees Two Lakh or both[38]. After ushering these veiled aspects to spotlight, it becomes evident that the Act does not palpably moot privacy and only its comprehensive exegesis exposes its masked constituents, *in conspectus omnium*; in our opinion, comprehending this concept *in effacacius* is the need of the hour.

Cyber Crime Laws in The United States of America (USA):

"The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution." [39]

Today, India is the second largest user of Internet in the world boasting 462 million people[40], implying a rise of 9,142.5% in its users, against the 200.9% of the United States of America which settled on the third spot this year[41]. The United States of America strives to cushion privacy through a combination of constitutional and legislative comments and self-regulations; resembling the *modus operandi* of the Indian Judiciary. Through its stern rules and regulations[42], this American Legislations house great number issues to define a "cybercrime" with respect to the invasion of privacy of the internet users. For instance, it is an offence to intentionally expropriate or utilize or reveal any hoarded information and the culprit is subject to fine or imprisonment upto 5 years or both[43],

unless the person/body carrying out the same is authorized to do so[44]. Likewise, the intentional ingress to stored data which exceeds the scope of authority would be declared as an unlawful offence and would be subject to punishment with imprisonment upto 5 years or fine or both or upto 10 years or fine or both (depending upon the offence so committed)[45]. And if a mortal knowingly conveys, possesses or manoeuvres without lawful authority, a means of identification of a person shall, be subjected to imprisonment upto 2 years *autem* to the punishment so accorded for such a felony[46]. Also, any person who knowingly and with the intention to defraud fabricates, wields or traffics in one or more counterfeit access to devices or acquires unaccredited access to the same shall be held to be invasive of privacy and be punished with an imprisonment upto 10 years or a fine or both[47]. These legislations endeavour to shelter the Government data and hence maintain its privacy, by explicitly mooting certain computers as "protected"[48] and any person knowingly accessing it without any authorization or exceeding the same and thus securing this information might injure the State would be granted a term of imprisonment upto 10 years and a fine or both[49]. Along the same lines, the intentional unauthorized access to any non-public computer or department or agency of The United States which might affect the State is a severe offence and the offender is subject to imprisonment upto one year or fine or both[50]. Violation of privacy in its truest sense is witnessed when a soul knowingly and intently traffics in the password to gain unauthorized access to the computer and is liable to liable to be punished with imprisonment up to 1 year or a fine or both. And to access a protected computer without authorization and intentionally commence the transmission of multiple commercial electronic mail messages from such a computer shall be punishable with imprisonment upto 3 years or a fine or both[51]. With respect to such austere laws, the effects of these legislations are amplified by the verdicts so given by the Honourable Courts of The United States of America. For instance, "*Officers must generally secure a warrant before conducting searches*" of cell phones of people who have been arrested in order to access the information so present inside it; lest, would be held violative of the person's privacy[52]. Likewise, the Courts call for strictly abiding by the rules which impose a duty upon the telecommunication carriers to safeguard the information which it receives or obtains from its customers, in accordance with Law[53]. Lastly, an unauthorized and hence illegal hacker if proven guilty is likely to be sentenced for a term of imprisonment upto 10 years or fine or both[54]. Thus, on a careful analysis of the two legislations, it becomes clear that they serve the same purpose, and are of the same nature. However, these legislations slightly cover more offences and impose stricter punishment upon the offenders, besides safeguarding privacy in the cyberspace in the most structured way possible, thereby promising to uphold the Fourth Amendment to their Constitution[55]- something which India needs to learn and imbibe with the changing times, in our opinion.

Conclusion:

Thus, in an era where the bulk of this nation is burdened with conflict of laws, this Act complements with the Constitution to uphold the Right to Privacy, if not concretely. In an eccentric way, it interprets violation of one's privacy as the "*unauthorized access to one's computer source*", which *quidem*, is its essence; endorsing the same by enforcing stern punishments to intercept the infraction of this right in the cyber space, rather unknowingly. One may argue that by cushioning the material itself, this Act harbours the privacy of the respective soul. However, the concept of privacy cannot be confined to a single point of view as multifarious genus of privacies *edoem*[56], of which this Act engulfs its physical[57] and

informational[58] forms. Henceforth, a thorough read concludes that the Act leaves no stone unturned to shelter one's privacy in the cyber space; though it is not its sole motive, must be acknowledged by the learned readers.

(Endnotes)

1 * I B.A.LL.B at ILS Law College, Pune
2 As retrieved from: (https://thewire.in/170303/supreme-court-aadhaar-right-to-privacy/)
3 1954 AIR 300, 1954 SCR 1077
4 1963 AIR 1295, 1964 SCR(1) 332
5
6 Article12 of Universal Declaration of Human Rights (UDHR). As retrieved from:(http://www.claiminghumanrights.org/udhr_article_12.html)
7 Supra 1
8 Government of India
9 Of its citizens
10 Who are active on database
11 In the cyber space
12
13 As retrieved from (http://www.datagovernance.com/quotes/privacy-security-quotes/)
14 As retrieved from (https://www.merriam-webster.com/legal/roght%20of%20privacy)
15 Freedoms; *Govind V. State of M.P.* [1975 SCC (2) 148]
16 Right to Life and Personal Liberty and to live with Dignity; *PUCL V. Union of India* [AIR 1997 SC568]
17 Especially the Fundamental Rights
18 Or both
19 Section 70 of the Information and Technology Act, 2000 (With 2008 Amendments).
20 Section 43(1)(a) of Information and Technology Act, 2000 (With 2008 Amendments)
21 Section 43(1)(b) of Information and Technology Act, 2000 (With 2008 Amendments)
22 Under this Act
23 Section 43(1)(a) of Information and Technology Act, 2000 (With 2008 Amendments)
24 Section 43(1)(d) of Information and Technology Act, 2000 (With 2008 Amendments)
25 Section 43(1)(a) of Information and Technology Act, 2000 (With 2008 Amendments)
26 Not explicitly mentioned in the Act, after the 2008 amendments
27 Section 43(1)(i) of Information and Technology Act, 2000 (With 2008 Amendments)
28 *Umashankar Shiva Subramanium V. ICICI Bank* [Petition No. 2462/2008]
29 (2005) F.S.R 38';119(2005) dlt 596; 2005 (30) PTC 437 DEL
30 Of the Director of Vigilance and Anti-Corruption (DVAC) in this case
31 *A. Shankar V. State Rep.* [Crl.O.P. No. 6628 of 2010]
32 Section 70 of Information and Technology Act, 2000 (With 2008 Amendments)
33 Section 70 of The Information and Technology Act, 2000 (With 2008 Amendments)
34 With respect to the Act, terrorism would mean leaking any information that might cause injury to the citizens or the sovereignty of the State: (Section 66F(A) AND 66F (B)
35 Section 66F(1) of The Information and Technology Act, 2000 (With 2008 Amendments)
36 Section 66F(2) of the Information and Technology Act, 2000,(With 2008 Amendments)
37 Section 66C of Information and Technology Act, 2000 (With 2008 Amendments)
38 Section 66E of the Information and Technology Act, 2000, (With 2008 Amendments)
39 Supra 1
40 As retrieved from: (https://www.statistia.com/statistics/262996/number-of-internet-users-in-selected-countries/)
41 As retrieved from: (http://www.internetworldstats.com/top20.htm)
42 Derived from various Act and Regulations
43 18 U.S.C § 2511
44 §2516, 2517
45 18 U.S.C § 2701
46 18 U.S.C § 1028A
47 18 U.S.C § 1029
48 And hence the data within it would be assumed to be protected. 18 U.S.C § 1030
49 18 U.S.C § 1030
50 18 U.S.C § 1030
51 18 U.S.C § 1037
52 Riley V. California [134 S. Ct. 2473, 2485 (2014)]
53 47 U.S. Code § 222-Privacy of customer information
54 As retrieved from: (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4083268/)
55 Fourth Amendment: "the right of people to be secure in their persons, houses, papers, and effects against unreasonable seizures and searches, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized". As retrieved from: (https://www.law.cornell.edu/wex/fourth_amendment)
56 As seen in (http://thelawdictionary.org/privacy/)
57 Right to be left alone physically (THE RIGHT TO PRIVACY (4 Harvard L.R.(Dec 15, 1890))
58 Data protection

Gender Justice: A Comparative Study of U.K., U.S.A., E.U. and India

[1*]Ms.Shivanjali Bhoite

Introduction

In most ancient societies women have been considered men's inferiors physically and intellectually. Throughout most of ancient Greece and Rome, women enjoyed very few rights. Marriages were arranged; women had no property rights and were not entitled to education. In ancient China, the yin and yang philosophy reinforced the notion of women's inferiority. The yang (male) always dominated the Yin (female). China also devised one of the most repressive customs of foot binding for women, rendering the woman uncomfortable and dependent on family and servants. According to Hindu laws of Manu as put forth in the ManuSmriti, women were subservient to male relatives, widow remarriage was not allowed and the law sanctioned the practice of Sati, a truly atrocious practice. Wearing bangles is also understood to be a form of fetters/shackles. Under common law of England, a married woman hardly had any rights; she had no rights to her property after marriage. In the early history of the United States, women and children were considered as a man's possession.

Over the centuries, as traditional patriarchal customs and laws became more deeply entrenched, women's lives became more restricted and oppressed. Most women were still denied education and their lives revolved around home making and managing. We still see this custom today in a lot of families. The main focus of this article is on gender customs and laws in the United States of America, United Kingdom, European Union and India.

THE THIRD GENDER:

The word 'Gender' in archaic use includes men and women only. But in recent times society has come to acknowledge transgender people (Hijras). This is also better known as the third gender. The term 'gender justice' denotes that all people having same or different gender will be treated with equality, justice and fairness and shall not be discriminated against on the basis of their gender. It is equality of all sexes.

GLOBAL VIEW ON GENDER JUSTICE

Equal participation by women and men in both economic and social development, and women and men benefiting equally from societies' resources is crucial for achieving gender justice.

The UNIFEM[2] (United Nations Development Fund for Women) was created in 1976 to provide technical and financial assistance for women's empowerment. The Convention on the Elimination of all forms of Discrimination against Women (CEDAW) was adopted in 1979 by the UNGA[3]. It is sometimes described as an international bill of rights for women. It is of significance that the United States is the only developed nation not to ratify this convention. The Decade for Women (1976-1985) and four world conferences on women (between 1975 and 1995) contributed significantly to raising awareness and commitment to gender equality and gender justice.

In July 2010, the United Nations General Assembly created UN Women, the United Nations Entity for Gender Equality and the Empowerment of Women. In doing so, UN Member States took an historic step in accelerating the Organization's goals on gender equality and the empowerment of women. Apart from that the Commission on the Status of Women, a global policy making body of ECOSOC[4] is dedicated exclusively to gender equality and advancement of women.

The UNDP[5] has developed the two most well-known gender justice indexes – Gender