International Journal of Pure and Applied Mathematics
Volume 120 No. 5 2018, 4067-4074
ISSN: 1314-3395 (on-line version)
url: http://www.acadpubl.eu/hub/
Special Issue

RIGHT TO PRIVACY IN DIGITALIZED INDIA

[1]SANTHOSH S , [2]Ms. Renuga C

[1]Student of Saveetha school of law, saveetha university, Saveetha Institute of Medical and Technical Sciences ,Chennai77, Tamil nadu , India.

[2]Assistant professor, saveetha school of law, saveetha university, Saveetha Institute of Medical and Technical Sciences ,Chennai77, Tamil nadu , India.

[1]Santosh.sivasankaran@gmail.com, [2]renugac.ssl@saveetha.com

Abstract:

This paper shall deal with the advent of privacy as a concept in India, relating to right to privacy in India and the effect that it would have on the Indian economy at large. This paper would like to specifically focus on right to privacy in digitalized India and the impact it could have on the citizens of India, especially considering a large number of people live in very technologically isolated areas, where a phone signal itself is hard to comeby, let alone an internet connection to access modern facilities such as net banking, etc. Therefore, it is important to note that the effects of right to privacy might reach everyone in the country, which inevitably leads to differing circumstances. With the advent of the Aadhar card, it is also important to note that the biometric data of every Indian citizen will be stored in one gigantic database, which would result in many safety issues that would pop up as a result of many potential cyber threats and other such issues. This paper shall deal with those potential threats, and truly gauge whether right to privacy will be enforced by the citizens of India.

Keywords: Digitalization, aadhar, privacy, data, security, cyber.

Introduction:

The present spotlight on the privilege to protection depends on some new substances of the computerized age. Individual spaces and securities that were already allowed basically by physical division are never again ensured. The computerized organize enters the most proximate spaces and difficulties the typically acknowledged ideas of the private. It brings into concentrate new methods for practicing social, financial, and political power, and lessening of autonomies. Like in the physical space, the private and people in general should

be isolated in the computerized domain too. We require an established definition and assurance of the privilege to uniqueness, individual self-governance and security in the advanced age. It must be given in the clearest terms by the Supreme Court, which is at present thinking about this issue. All such roles of the state must be constitutionally circumscribed, with strict laws. While establishing a right to privacy, the Supreme Court must also direct the state to develop appropriate institutions for shaping the state's role in a digital society/economy. This may require, at some stage, an independent branch of the state exclusively dealing with data issues and management. Confining of a privilege to security must not reduce the state's expected part in our aggregate computerized prospects. This will just guarantee that worldwide advanced partnerships turn out to be almighty financial, social and political performing artists. They as of now give the majority of the advanced administrations that give off an impression of being of an open amicableness, and thus control and shape whole areas. The aim of this study is to compare right to privacy before and after digitalization, and to observe if right to privacy is being followed and enforced by the people of India.

Research Methodology:

This paper will use a non-empirical, doctrinal form of research using secondary sources as the main source of data. Secondary sources such as books, journals, research papers and court judgements will be used to support the claims made in this paper. The gap that this paper will try to fill is whether digitalized India concept affects right to privacy or not.

Supreme Court Judgement:

On 21st of August, 2017, the nine-judge seat of India's Supreme Court has recently decided that "protection is characteristic for opportunity of life and individual freedom" ensured in Article 21 of the Constitution of India and qualifies as "a primal common right". The Court has underscored that its undertaking was to "give established significance to singular freedom in an interconnected world". The judgment tries to expand a thought of protection with extraordinary consideration regarding "mechanical advance" that has rendered our "lives open to electronic investigation." The protracted content connects with the good and lawful inquiry of protection. Be that as it may, law in advanced circumstances should likewise think about the material parts of protection, and the social and monetary outcomes of particular mechanical models and how they emerge/damage/regard security. Security or its scarcity in that department is incorporated in with the outline of techno antiquities and winds up embroiled specifically courses with specific arrangements of

computerized stuff. The Honourable Court has recognized that "electronic tracks contain capable methods for data" and consequently protection concerns are a major issue "in the period of data". Be that as it may, the judgment is just a start. The true appearances of the privilege to security in the advanced age will depend especially on standards improvement by the administration, and decisions of the courts, in regard of the solid plan of the computerized. As we proclaim the notable judgment, we have to advise ourselves that the genuine assignment lies ahead. The bench comprised Chief Justice Khehar and Justices J. Chelameswar, S.A. Bobde, R.K. Agrawal, Rohinton Nariman, A.M. Sapre, D.Y. Chandrachud, Sanjay Kishan Kaul and S. Abdul Nazeer.

Landmark Cases regarding right to privacy:

District Registrar and Collector, Hyderabad and another v. Canara Bank and another (2004). This Supreme Court judgment refers to personal liberty, freedom of expression and freedom of movement as the fundamental rights that further gives rise to the right to privacy. Petronet LNG LTD vs. Indian Petro Group and Another (2006). This was before the Delhi HC and it was established that firms cannot assert a fundamental right to privacy. Selvi and others v. State of Karnataka and others (2010). Interestingly, the SC made a difference between physical privacy and mental privacy. The case also established a connection of the right to privacy with Article 20(3) (self-incrimination). Unique Identification Authority of India & Anr. v. Central Bureau of Investigation (2014). The Central Bureau of Investigation sought access to the huge database complied by the Unique Identity Authority of India for the purposes of investigating a criminal offence. The SC, however, said that the UIDAI was not to transfer any biometrics without the consent of the person.

Justice K.S. Puttuswamy (Retd.) & Anr. v. Union of India & Ors. (2015). The Unique Identity Scheme was discussed along with right to privacy. The question before the court was whether such a right is guaranteed under the Constitution. The attorney general of Indian argued that it privacy is not a fundamental right guaranteed to Indian citizens

Privacy and the materiality of technology design:

Specific outline highlights of an innovation open up specific regulating and moral issues and difficulties relating to security. The promotion based model of the Internet depends on an exploitative, 'access-for-information' arrange at the base of the worldwide reconnaissance administration. It empowers free-of-cost access to online data and correspondence administrations for clients, while in the meantime eating up relentlessly all of their own data. Stages and their terms of administration control the degrees of protection,

constantly guaranteeing access to client information of course. In an examination investigation of 26 security applications for ladies, it was discovered that every one of them, incidentally, need arrangements for protection or terms of utilization, in this manner involving a high danger of conceivable information and fraud and unfortunate reconnaissance of clients. Each improvement in computerized innovation that turns out to be a piece of our social texture compels us to go up against another inquiry concerning the material outline of protection. The organization between Google's Deep Mind and National Health Service UK uncovers that brought together data frameworks end up helpless against ruptures, notwithstanding information insurance law and utilize confinement rules. The approach of individual advanced associates has introduced indirect access pathways through which recorded discussions are radiated back to equipment producers. Automatons for home conveyances are examining clients' homes to outline retail openings, and because of shrewd information and IoT improvements, gadgets converse with each other, without human intervention. In the data age reality, approaches or laws as for protection, for example, the 'notice and gathering' guideline, are in this manner rendered out of date. The hard code of advanced advances additionally appears to take the level headed discussion on the plain thought of security to new edges. Headways in Big Data examination empowered by subjective figuring upgrade the danger of social profiling and separation for individuals from underestimated networks. As a few researchers put it, "the sheer number and lavishness of databases and the expanding advancement of calculations" elevates not simply singular weakness to state and corporate observation, yet in addition endangers the educational security of whole social gatherings. In any case, we are a long way from laws to oversee calculations or Artificial Intelligence. Security must be rethought likewise as an aggregate right (PDF), and not only an individual one. In the particular decisions of techno-plan made to discharge apportions for the poor through biometric check, the current Aadhaar-based framework, which utilizes ID numbers to track clients of an expanding number of taxpayer supported organizations, takes away control that an individual has over their own particular biometric information. Rather, it opens them to the danger of wholesale fraud, borne out by numerous tales from various parts of the nation. As has been brought up, it was very conceivable to decide on a plan that was more decentralized through shrewd cards (PDF), with all the individual information held by singular recipients themselves. Yet, the civil argument is regularly displayed as fait accompli – to be poor, doubtlessly, is to do without the privilege to security.

Interpreting the 'proportionality of interference' principle:

Iiation space under the RTI Act. There was no rupture or spillage of Aadhaar information from UIDAI database or server as has been circulated by the said report. UIDAI said that acting instantly on this, UIDAI and the Ministry of Electronics and IT had coordinated the concerned government divisions/services to quickly expel it from their sites and guarantee that such infringement don't happen in future. Certain different measures were additionally taken at different levels to guarantee that such episodes of show of Aadhaar numbers don't happen. Following UIDAI's activity such information were expelled from these sites promptly. Be that as it may, the news introduced the actualities in a skewed way and misdirects perusers as though Aadhaar information has been spilled or broken at 210 sites posturing Aadhaar security is defenceless. UIDAI emphasized that Aadhaar security frameworks are best of the worldwide gauges and Aadhaar information is completely secure. There has been no break or spillage of Aadhaar information at UIDAI. Additionally, the Aadhaar numbers which were made open on the said sites don't represent any genuine danger to the general population as biometric data is never shared and is completely secure with most elevated encryption at UIDAI and insignificant show of statistic data can't be abused without biometrics. UIDAI illuminated that the Aadhaar number is definitely not a mystery number. It is to be imparted to approved organizations when an Aadhaar holder wishes to profit a specific administration or advantage of government welfare plot/s or different administrations. Be that as it may, that does not imply that the correct utilization of Aadhaar number represents a security or money related risk. Likewise, insignificant accessibility of Aadhaar number won't be a security danger or won't prompt budgetary/other misrepresentation, with respect to an effective verification unique mark or iris of individual is additionally required. Promote all verifications occur within the sight of faculty of individual specialist co-op which additionally add to the security of the framework.

Conclusion:

Right to privacy has made leaps and bounds in the world of digitalized India, however, there always exists the possibility that things could go in harm's way if there ever was a security breach. However, with the implementation of cyber laws and cyber crimes in India, it does not seem like anything short of a terrorist attack on the databases that the Indian government holds all the biometric data that aadhar stores will ever be stolen. As a result, right to privacy is being protected by the government of India.

References

1) Anubhav Khamroi et Anjoy Shrimuktau, the curious case of right to privacy in India, O.P Jindal Global University
2) Raja Siddharth Raju et al, Aadhar card:- challengers and impact on digital transformation, Manav Rachna International University
3) Tanwar R, Railway reservation by Aadhar Card, procedia compute science, 20155
4) Greenleaf G, Confusion as India Supreme Court compromises on data privacy and ID number, privacy law and business report 2015
5) Otto M, The Right to privacy in employment, Bloomsbury, United States of America, p.p (13-16)
6) Ravinder Kumar, The right to privacy in India, concept and evolution, 2016
7) Nidhi Hazden, leftm right and centre, the idea of India, 2016
8) G Bhatia, State surveillance and right to privacy, 26 (5), National Law School review 127, 31 p, May 2015
9) Amber Sinha, Fundamental Right to Privacy-1, the centre for internet and society
10) Amber Sinha, Fundamental Right to Privacy-2, the centre for internet and society
11) Amber Sinha, Fundamental Right to Privacy-3, the centre for internet and society
12) Aashith Singh, et Nilesh Cochery, Right to Privacy and data protection, Nishith Desai and Associates
13) Sabreen Ahmed, Right to Privacy, Is UIDAI a violation? The world journal of juristic policy, ISSN
14) Buddenhudi Halder, Privacy in the age of big data
15) Laney D, 3D management control by data volume, meta group research
16) Morz N, Big date:- principles, New York, Manning publication
17) Kathy Furgiay et Frank Guttai, understanding your right to privacy, rosen publishing group, ie, p3
18) Bijan Bahabatt, Position and perspective of privacy law, NLU Gujarat
19) Warren S and Branders, 2000, the right to privacy, Harvard Law review
20) K.S. Puttusamy vs Union of India
21) Dr.Lakshmi T and Rajeshkumar S , March 2018. "In Vitro Evaluation of Anticariogenic Activity of Acacia Catechu against Selected Microbes", International Research Journal of Multidisciplinary Science & Technology, Volume No. 3 , Issue No. 3, P.No 20-25.

22) Trishala A , Lakshmi T and Rajeshkumar S, April 2018.“ Physicochemical profile of Acacia catechu bark extract –An In vitro study”, International Research Journal of Multidisciplinary Science & Technology, Volume No. 3 , Issue No. 4, P.No 26-30.