

RIGHT TO PRIVACY AND INVASION OF PRIVACY- WITH REGARD TO AADHAAR- AN OVERVIEW

¹R.RAMASAMY

¹Student Of Law, Saveetha School Of Law, Saveetha Institute Of Medical And Technical Sciences,
Saveetha University,Chennai-77, Tamilnadu,India.

²PROF Dr.A. SREELATHA

²Saveetha School Of Law, Saveetha Institute of Medical and Technical Sciences,Saveetha
University,Chennai-77, Tamilnadu,India.

¹ramasamylegaladvisor@gmail.com, ²annamanenisreelatha.ssl@saveetha.com

ABSTRACT

The collection of personal information through highly portable means is becoming increasingly popular throughout numerous governments and businesses³, for example, through the use of smart cards, radio frequency identification (RFID) tags and ID cards. However, there are many fears concerning these information collecting technologies, in particular related to privacy. The aspect of general right of privacy with which the present study is principally concerned, since it is the one which has been the most profoundly affected, and some would say most dangerously threatened by recent developments in information technology. Technological advances in visual and aural surveillance is that issues of invasion of privacy by surveillance become issues of 'information privacy'. Deprivation means a taking away of a constitutional right.

KEYWORDS

Aadhaar- privacy- article 21- constitution- UIDAI- information- data protection

INTRODUCTION

Privacy is a constitutionally protected right which not only emerges from the guarantee of life and personal liberty in Article 21 of the constitution, but also arises in varying contexts from the other facets of freedom and dignity recognised and guaranteed by the fundamental rights contained in Part III of the Indian constitution. Privacy is intrinsic to life, liberty, freedom and dignity and therefore, is an inalienable natural right. “Life and personal liberty are inalienable rights. These are rights which are inseparable from a dignified human existence. The dignity of the individual, equality between human beings and the quest for liberty are the foundational pillars of the Indian constitution. Life and personal liberty are not creations of the constitution. These rights are recognised by the constitution as inhering in each individual as an intrinsic and inseparable part of the human element which dwells within.”

AIM OF THE STUDY

The aim of this paper is to study the concept right to privacy, data protection and Aadhaar.

RESEARCH QUESTION

WHETHER AADHAR CAN BE MADE MANDATORY AS SUPPORTING DOCUMENT AND HOW FAR PERSONAL DATA OF EVERY CITIZEN IS PROTECTED?

OBJECTIVES

- To understand the concept of Right to privacy.
- To analyze the role of Aadhaar in detail.
- To establish substantial arguments supported by law.
- To know about the consequences.
- To identify the threat to data protection.

HYPOTHESIS

NULL HYPOTHESIS- Right to privacy is not a fundamental right.

ALTERNATE HYPOTHESIS- Right to Privacy is a fundamental right.

RESEARCH METHODOLOGY

Only secondary sources have been referred for this study. The primary sources include interviews with the people were not possible. Secondary sources include books related to Constitutional law and research articles on the right to privacy and aadhaar.. Ample websites and blogs have also been referred for this study. This paper was completed through descriptive methodology.

PRIVACY

Professor Arthur Miller put it even more briefly, defining it as “the individual’s ability to control the circulation of information relating to him.”⁴ The general idea of “private” can be conceptualized as the practices or acts which we want to protect from public scrutiny.⁵ “Privacy” is a notoriously difficult concept to define and cannot be understood as a static and one-dimensional concept. It can only be construed as a group of rights.⁶ The said right has attracted different interpretations, the most important of which is the “notion of personhood”. *Jed Rubenfield* tried to conceptualize the notion of personhood as “some acts, faculties or qualities which are so important to our identity as [persons-as-human beings] that they must remain inviolable.”⁷ Privacy has also been considered a “type of social isolation”⁸; “right against unwarranted intrusion by the state”⁹; a “right against the intrusion on an individual’s personal life or affairs”¹⁰. Privacy includes at its core the preservation of personal intimacies, the sanctity of family life, marriage, procreation, the home and sexual orientation. Privacy also connotes a right to be left alone. Privacy safeguards individual autonomy and recognises the ability of the

⁴ Miller, A.R (1971), *Assault on Privacy: Computers, Data Banks and Dossiers*, Ann Arbor, Mich : University of Michigan Press, p.40.

⁵ 1 CANNATA, J.A., *THE INDIVIDUAL AND PRIVACY* (Routledge 2015)

⁶ J. L. MILLS, *THE LOST RIGHT* 4 (Oxford University Press 2008)

⁷ Jed Rubenfield, *The Right to Privacy*, 102 HARV. L. REV. 737, 740 (1989)

⁸ MANNHEIM, KARL & JOHN STEPHEN EROS, ED., *AN INTRODUCTION TO THE STUDY OF SOCIETY BY KARL MANNHEIM* (Literary Licensing, LLC 2013)

⁹ 2 BASU, DURGA DAS, *COMMENTARY ON THE CONSTITUTION OF INDIA* 4772 (3rd ed. Lexis Nexis 2016)

¹⁰ GREAT BRITAIN AND DAVID CALCUTT, *THE CALCUTT REPORT OF THE COMMITTEE ON PRIVACY AND RELATED MATTERS* 7 (Stationery Office Books 1970).

individual to control vital aspects of his or her life. Personal choices governing a way of life are intrinsic to privacy. Privacy protects heterogeneity and recognises the plurality and diversity of our culture. While the legitimate expectation of privacy may vary from the intimate zone to the private zone and from the private to the public arenas, it is important to underscore that privacy is not lost or surrendered merely because the individual is in a public place. Privacy attaches to the person since it is an essential facet of the dignity of the human being.” It is privacy which is a powerful guarantee if the state were to introduce compulsory drug trials of non-consenting men or women. The sanctity of marriage, the liberty of procreation, the choice of a family life and the dignity of being are matters which concern every individual irrespective of social strata or economic wellbeing. The pursuit of happiness is founded upon autonomy and dignity. Both are essential attributes of privacy which makes no distinction between the birth marks of individuals. Right to privacy is a basic fundamental right. It forms an intrinsic part of Art. 21 and freedoms guaranteed in Pt. III. It permeates core of Preambular philosophy underlying “liberty” and “dignity” as also human concepts of “life” and “personal liberty” enshrined in Art. 21 and wide ranging freedoms guaranteed under Pt. III, considered essential for a meaningful human existence. It also finds recognition in various international conventions as well as in Protection of Human Rights Act, 1993. Absence of express enumeration of right to privacy is no ground for disregarding its omnipresence in Pt. III. Its three connotations viz. spatial control, decisional autonomy and informational control are significant. It has a normative as well as descriptive function and negative as well as positive content. It has intrinsic as well as instrumental value. It comprehends physical as well as mental aspects. Merely because a precise definition cannot be formulated, it cannot be termed as vague and on that ground cannot be disregarded as a fundamental right.¹¹

NEED FOR E-GOVERNANCE

Long before the public Internet came into being in the early 1990s, governments across the world have moved to standardise and centralise records about their citizens. As computing power increased and became cheaper, states were able to make increasing efficiency gains within their bureaucracies by centralising and standardising information about citizens.¹² In accordance with

¹¹ K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1

¹² For a discussion on the importance of computing to modern states and societies see Robertson, D.S. (1998) *The New Renaissance: Computers and the Next Level of Civilization*. Oxford University Press, United States of America

the views of James C. Scott, states have sought to make the societies they govern 'legible' in order to promote their policies.¹³ They also serve to respond to persistent demands on public bureaucracies to cut costs by increasing efficiency through computerisation. These efficiency gains have often had the effect of negatively impacting on citizens' privacy and anonymity. Public initiatives to create large public databases about citizens have been met with scepticism by privacy advocates. The dangers of such databases are particularly evident when the information is lost. Such databases and identification services often include an online component, allowing citizens to access various government services via the Internet. Use of these services may provide many benefits to citizens, such as greater convenience and efficiency. "These benefits, however, do not come without a cost: the loss of privacy. Privacy in this context means 'information privacy,' an individual's claim to control the terms under which personal information – information identifiable to an individual – is acquired, disclosed and used."¹⁴ This prescient statement describes precisely the difficulty in ensuring that eGovernment is both effective and guarantees privacy. This tension can also be found in more recent forms of eGovernment. Typically these initiatives attempt to increase participation of citizens and the transparency of government operations, however here too there may be privacy concerns. For one, users participating in these initiatives are typically required to identify themselves as citizens in participative government initiatives, as non-citizen participation is typically not possible. Moreover they are expected to participate in these initiatives with their 'whole identity.' Anonymous or pseudonymous participation – even for individuals identified as citizens – is generally not an option. Another important point is the tension between transparency and open Government or participatory government initiatives and privacy. Most participatory governmental initiatives require high levels of transparency to ensure the legitimacy of the process. However by doing so they run the danger of overly restricting the rights of individuals to their personal data in order to safeguard transparency. It is important to consider the close cooperation with the private sector in many eGovernment and open Government initiatives. As governments often do not have the capacity to perform these functions themselves, they frequently outsource processes and services integral to modern governments to private service

¹³ Scott, J.C. (1998) *Seeing like a state : how certain schemes to improve the human condition have failed*. New Haven: Yale University Press.

¹⁴ Gates, J., & Privacy Working Group. (1995). *Privacy and the National Information Infrastructure: Principles for Providing and using Personal Information*. Information Policy Committee, Information Infrastructure Task Force. Retrieved from <http://aspe.hhs.gov/datacncl/niiprivp.htm>.

providers. While this may be an effective way of cutting costs, it also provides additional privacy risks by involving third parties in the processing, transfer and storage of citizens' personal data. These interactions with the private sector do not necessarily harm citizens' privacy, but they do introduce an additional layer of complexity that needs to be governed appropriately.

CONSTITUTION OF INDIA AND RIGHT TO PRIVACY

To live is to live with dignity. The draftsmen of the constitution defined their vision of the society in which constitutional values would be attained by emphasising, among other freedoms, liberty and dignity. Dignity is the core which unites the fundamental rights because the fundamental rights seek to achieve for each individual the dignity of existence. Privacy with its attendant values assures dignity to the individual and it is only when life can be enjoyed with dignity can liberty be of true substance. The draftsmen of the constitution had a sense of history— both global and domestic— as they attempted to translate their vision of freedom into guarantees against authoritarian behavior. The backdrop of human suffering furnished a reason to preserve a regime of governance based on the rule of law which would be subject to democratic accountability against a violation of fundamental freedoms. Hence, it would be an injustice both to the draftsmen of the constitution as well as to the document which they sanctified by constricting its interpretation to an originalist interpretation. The object of Article 21 is to prevent encroachment upon personal liberty by the executive, save in accordance with law.¹⁵ Article 21 is a declaration of deep faith and belief in human rights. In this “pattern of guarantee woven in Chapter III of this Constitution, personal liberty of man is at root of Article 21 and each expression used in this Article enhances human dignity and values. It lays foundation for a society where rule of law has

¹⁵ G.Gurunadha Reddy v. A.P.Road Transport Corporation, AIR 1999 AP 179.

primary and not arbitrary or capricious exercise of power.¹⁶ It was held that the term is used in this Article 21 as a compendious term to include within itself all varieties of rights which goes to make up the “personal liberties” of man other than those dealt within several clauses of Article 19(1). While Article 19(1) deals with particular species or attributes of that freedom, “personal liberty” in Article 21 takes on and comprises the residue.¹⁷ The law and procedure authorizing interference with personal liberty and right to privacy must also be right, just and fair and not arbitrary, fanciful or oppressive.¹⁸ In *A.K.Gopalan v. State of Madras*¹⁹, which held that certain Articles in the constitution exclusively deal with specific matters and in determining whether there is infringement of the individual’s guaranteed rights, the object and the forms State action alone need to be considered and the effect of the laws on the fundamental rights of the individuals in general will be ignored, was held as not correct. A person is entitled to enjoy his personal rights and to be protected from encroachments on such personal rights, freedoms and liberties. Any action taken which may create hazards of life will be encroaching upon the personal rights of a citizen to enjoy the life according to law.²⁰ Right to privacy, though not expressly provided in the constitution, still it can be traced from the ‘right to life’ in Article 21.²¹ Right to privacy was implied within right to speech and further it could be gathered from the entirety of fundamental rights in the Constitutional schemes. The right is not absolute and are subject to reasonable restrictions and the same can be denied only when an important countervailing interest is shown to be superior.²² In *R.Rajagopal v. State of T.N*²³, held that right to privacy is implicit in the right to life and liberty guaranteed under Article 21. The above principle has now been accepted in *People’s Union for Civil Liberties v. Union of India*. An interference with privacy is not even like an elephant of which it can be said it is at least easy to recognize if not to define. The meaning of privacy can be influenced by the context in which it appears.²⁴ In *A.K.Gopalan v. State of Madras*,²⁵ which held that certain Articles in the

¹⁶ Kartar Singh v.State of Punjab (1994) 3 SCC 569.

¹⁷ Kharak Singh v. State of U.P., AIR 1963 SC 1295: (1964) 1 SCR 332.

¹⁸ District Registrar and Collector, Hyderabad v. Canara Bank, AIR 2005 SC 186 : (2005) 1 SCC 496.

¹⁹ (1950) SCR 88.

²⁰ People’s union of civil liberties v. Union of India AIR 1997 SC 568 : (1997)1 SCC 301; Sunil Batra v. Delhi Administration AIR 1980 SC 1579 : (1980) 3 SCC 488; Valsamma Paul v. Cochin University (1996) 3 SCC 545.

²¹ Kharak Singh v. State of U.P., (1964) 1 SCR 332: AIR 1963 SC 1295.

²² Gobind v. State of M.P., (1975) 2 SCC 148 : AIR 1975 SC 1378 : (1975) 3 SCR 946

²³ (1994) 6 SCC 632 : AIR 1995 SC 264.

²⁴ R. v. Broadcasting Standards Commission, (2000) 3 All ER 898.

Constitution exclusively deal with specific matters and in determining whether there is infringement of the individual's guaranteed rights, the object and the form of State action alone need to be considered and the effect of the laws on the fundamental rights of the individuals in general will be ignored was held as not correct. The refrain that the poor need no civil and political rights and are concerned only with economic well-being has been utilised through history to wreak the most egregious violations of human rights. Above all, it must be realised that it is the right to question, the right to scrutinise and the right to dissent which enables an informed citizenry to scrutinise the actions of government. Those who are governed are entitled to question those who govern, about the discharge of their constitutional duties including in the provision of socio-economic welfare benefits. The theory that civil and political rights are subservient to socio-economic rights has been urged in the past and has been categorically rejected in the course of constitutional adjudication by this court. The constitution was not the sole repository of the right to life and liberty. The recognition of the right to life and personal liberty under the constitution does not denude the existence of that right, apart from it nor can there be a fatuous assumption that in adopting the constitution, the people of India surrendered the most precious aspect of the human persona, namely, life, liberty and freedom to the state on whose mercy these rights would depend. Such a construct is contrary to the basic foundation of the rule of law which imposes restraints upon the powers vested in the modern state when it deals with the liberties of the individual. The power of the court to issue a Writ of Habeas Corpus is a precious and undeniable feature of the rule of law. A constitutional democracy can survive when citizens have an undiluted assurance that the rule of law will protect their rights and liberties against any invasion by the state and that judicial remedies would be available to ask searching questions and expect answers when a citizen has been deprived of these, most precious rights. In the Indian context, Sen points out that the Bengal famine of 1943 "was made viable not only by the lack of democracy in colonial India but also by severe restrictions on reporting and criticism imposed on the Indian press, and the voluntary practice of 'silence' on the famine that the British-owned media chose to follow". Political liberties and democratic rights are hence regarded as 'constituent components' of development.²⁶ Development cannot really be seen merely as the process of increasing inanimate objects of convenience, such as raising the

²⁵ (1950) SCR 88.

²⁶ Sen's classic *The Idea of Justice* (Penguin Books, 2009)

GNP per head, or promoting industrialization or technological advance or social modernization. These accomplishments are, of course, valuable – often crucially important – but their value must depend on what they do to the lives and freedoms of the people involved. For adult human beings, with responsibility for choice, the focus must ultimately be on whether they have the freedom to do what they have reason to value. In this sense, development consists of expansion of people's freedom.²⁷

AADHAAR

The Aadhaar act attempts to create a method for identification of individuals so as to provide services, subsidies and other benefits to the residents of the country. While the effectiveness of Aadhaar to the extent claimed in preventing leakages in social welfare schemes has been questioned, the advantages of computerization and reliably maintaining eligibility and distribution records in digital forms are well accepted. Any digitization requires indexes or unique ids, and in social welfare schemes local unique ids like ration or job card numbers are typically used. Standardizing the digital record keeping processes across geographies and verticals, and linking the local ids with the unique national identities provided by Aadhaar, tantamount to virtually collating the different digital record tables into one. Though the digital records may still be geographically distributed, real-time access to the data, using the Aadhaar ids as handles, can then be provided to authorized central and state agencies for audit, monitoring, analysis and planning purposes. Thus, the Aadhaar number provides a single index across all services that may use Aadhaar. The Unique Identification Authority of India (UIDAI) is responsible for providing the basic identification and authentication services. It provides a unique identifier (Aadhaar number) to each resident and maintains their biometric and demographic data in a Central Identities Data Repository (CIDR). The UIDAI manages the CIDR and provides identification and authentication services with yes/no answers. An Authentication User Agency (AUA) who provides services to users that are successfully authenticated. Thus, an AUA connects to the CIDR and uses Aadhaar authentication to validate a user and enable its services. Examples of AUAs and services are banks, various state and central government ministries providing services such as the Public Distribution System (PDS), the National Rural Employment Guarantee Scheme (NREGS), and even private agencies like mobile

²⁷ Sen's writings in *The Country of Young Boys* (Oxford University Press, 2015)

phone operators. The responsibility of logistics of service delivery rests with the AUAs. In this federated model an AUA may choose to use only Aadhaar identification, or also authentication in conjunction with their own legacy identification and authentication systems. An AUA is required to enter in to a formal contract with UIDAI to be able to use Aadhaar authentication services. An Authentication Service Agency (ASA) is an entity that has a secure leased line connectivity with the CIDR. ASAs transmit authentication requests to CIDR on behalf of one or more AUAs. An ASA enters into a formal contract with UIDAI. The users, namely, the residents of the country who enrol themselves with UIDAI and are issued unique identification numbers (Aadhaar numbers). A user has to present this number as the basic identification to an AUA for availing Aadhaar authentication services. The Aadhaar number for a user is common across all AUAs and service domains. The Point of Sale (POS) device, also known as authentication device which collects personal identity data from Aadhaar holders, prepares the information for transmission, transmits the authentication packets for authentication and receives the authentication results. An Enrolment Station, which is a collection of field devices used by enrolment agencies appointed by UIDAI to enrol people in to the Aadhaar database and capture their demographic and biometric particulars. Last date for linking of Aadhaar with bank account, mobile number and social welfare schemes, having been extended in earlier order to 31-3-2018, further extended till matter finally heard and decided by Court. Further, said interim order would also govern Passports (First Amendment) Rules, 2018.²⁸

Control of Personal Information²⁹- A right to restrict the use of ‘personal’ or ‘private’ information about an individual is central to the right to privacy. A large volume of such information is held by public bodies and is, potentially, open to misuse. The extent to which the use of this information is controlled or restricted is one of the most important ‘privacy’ issues.

Correlation of identities across domains: It may become possible to track an individual’s activities

across multiple domains of service (AUAs) using their global Aadhaar ids which are valid across these domains. This would lead to identification without consent.

²⁸ K.S. Puttaswamy v. Union of India, (2018) 4 SCC 651

²⁹ Westin: R wacks, The Protection of Privacy (Sweet & Maxwell, 1980).

Identification without consent using Aadhaar data: There may be unauthorized use of biometrics to illegally identify people. Such violations may include identifying people by inappropriate matching of fingerprint or iris scans or facial photographs stored in the Aadhaar database, or using the demographic data to identify people without their consent and beyond legal provisions.

Illegal tracking of individuals: Individuals may be tracked or put under surveillance without proper authorization or legal sanction using the authentication and identification records and trails in the Aadhaar database, or in one or more AUA's databases. Such records will typically also contain information on the precise location, time and context of the authentication or identification, and the services availed.

Possible measures against insider attacks

Our starting point is that the environment in which the CIDR programs (code) are executed cannot be assumed as trusted. One must address the possibility that the attacker has full access to the computer programs that may be running on the UIDAI database. This may include both the source code and the runtime environment. How can one hope to secure such a system against insider attacks? We believe that two independent lines of defence are required:

1. There has to be an independent third party that can play the roles of an auditor and a keeper of cryptographic keys.
2. Several modern tools and techniques from computer science offer (partial) solutions to these problems.

These need to be studied, evaluated and appropriately deployed.

WHAT IS BIOMETRICS?

While the word "biometrics" sounds very new and "high tech," it stands for a very old and simple concept—human recognition. In technical terms, biometrics is the automated technique of measuring a physical characteristic or personal trait of an individual and comparing that characteristic or trait to a database for purposes of recognizing that individual.³⁰ Consistently has

³⁰ B. Miller, "Everything you need to know about automated biometric identification," Security Technol. Design, Apr. 1997.

held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.³¹

BIOMETRICS- IRIS AND RETINA

While both the iris and retina contain medical information, it is by no means obvious that biometric scanning of the iris or retina automatically implicates privacy concerns related to the disclosure of medical information. A necessary area of further technical inquiry is whether the computerized bytecode taken of the iris or retina actually contains this medical information or if the information captured is sufficient to be used for any type of diagnostic purpose. While much research remains to be done, the availability of such information, with its possible links to medical information, raises important questions about the privacy aspects of the information disclosed.

The Loss of Anonymity and Autonomy: A basic criticism of biometrics from the standpoint of privacy is that we, as individuals, lose our anonymity whenever biometric scanning systems are deployed. Controlling information about ourselves includes our ability to keep other parties from knowing who we are. While we all know that at some level, a determined party—whether the state or a private actor—can learn our identity (and much more about us), biometric scanning makes it plain that our identity is now fully established within seconds. As Prof. Clarke explains, “The need to identify oneself may be intrinsically distasteful to some people, they may regard it as demeaning, or implicit recognition that the organization with whom they are dealing exercises power over them”. the loss of anonymity leads to an inevitable loss of individual autonomy. In the present service economy, information has become an increasingly valuable commodity. The computer has exacerbated this problem through its capacity to disclose a large amount of personal information to a large number of unrelated individuals in a very short amount of time.³² Public- and private-sector organizations already have the ability to gather substantial amounts of information about individuals by tracking, for example, credit card use, consumer spending, and demographic factors. Biometrics, in combination with impressive advancements in computer and related technologies, would enable the state to monitor the actions and behavior of its citizenry. Privacy rights would be seriously at risk as technological advances become generally

³¹ Smith v. Maryland, 442 U.S. 735 (1979)

³² P. Mell, “Seeking shade in a land of perpetual sunlight: Privacy as property in the electronic wilderness,” Berkeley Technol. Law J., vol. 11, p. 1, 1997

disseminated and available to society.³³ In *Bowen v. Ray*, a leading Supreme Court case dealing with this issue, a Native American objected to the provision of an SSN for his minor daughter's application for welfare assistance as a violation of the family's religious beliefs. The court refused to sustain this challenge.³⁴ While critics of biometrics contend that this new technology is privacy's foe, the opposite, in fact, is true. Biometrics is a friend of privacy whether used in the private or public sectors. Biometrics proves itself as privacy's friend when it is deployed as a security safeguard to prevent fraud. Biometrics becomes a staunch friend of privacy when the technology is used for access-control purposes, thereby restricting unauthorized personnel from gaining access to sensitive personal information. The same biometric systems can be used for almost any information database (including databases containing biometric identifiers) to restrict or compartmentalize information based on the "need to know" principle. Biometrics also protects information privacy to the extent that it can be used, through the use of a biometric logon explained above, to keep a precise record of who accesses what personal information within a computer network. For example, individual tax records would be much better protected if an IRS official had to use his biometric identifier to access them, knowing that an audit trail was kept detailing who accessed which records. Far less snooping by curious bureaucrats would result. Beyond protecting privacy, biometrics can be seen as enhancing privacy.

NATIONAL ID CARDS IN UNITED KINGDOM

A government agency would tell you to report with existing documents (e.g. birth certificate, passport, national insurance number) to a named processing centre at a specified time. You would need to allow yourself to be fingerprinted, have your iris scanned and your photograph taken. If you did not attend, or if you did not allow your biometric data to be recorded, you would be fined up to £2500.

PRIVACY IN INTERNATIONAL CONTEXT

The ICJ study of 1972 quoted Professor Alan Westin's landmark book, *Privacy and Freedom*, in saying that privacy is at the heart of freedom in the modern state.³⁵ Professor David Flaherty has

³³ D. Mintie, "Report from Connecticut," Biometrics in Human Services User Group Newsletter, Mar. 1997

³⁴ *Bowen v. Ray*, 476 U.S. 693 (1986).

³⁵ Westin, A.F., *Privacy and Freedom*, p.350, Newyork: Atheneum (1967); London : Bodley Head (1970).

said that ‘Although privacy is an important instrumental value, it is not identical to such fundamental values as liberty, freedom and democracy.’³⁶ In much of Europe, protection of privacy tends to be intimately tied to protection of dignity and honor. It is often perceived as valuable not just for individual persons but society generally, particularly for maintaining civility, pluralism and democracy. Americans, however, tend to see privacy as important primarily in ensuring freedom from government intrusion. Differences occur even at the terminological level. American discourse on the fears raised by the misuse of computer technology has tended to resolve around the term ‘privacy’. By contrast, European discourse has tended to employ the more colorless appellation ‘data protection’.³⁷ The UN General Assembly adopted a set of guidelines on privacy and data protection in resolution 45/95 of 14 December 1990.³⁸ The first UN initiative dealing directly with privacy and data protection was a 1986 General Assembly Resolution insisting the UN Secretary-General to examine the impact of technological developments on human rights, including consideration of individuals’ right to privacy in the light of advances in recording and other techniques.³⁹ The quest and need for privacy is a natural one, not restricted to man alone, but arising in the biological and social processes of all the higher forms of life. All animals have a need for temporary individual seclusion or the intimacy of small units, quite as much as for the stimulus of social encounters among their own species. Indeed the struggle of all animals, whether naturally gregarious or not, to achieve a balance between privacy and participation is one of the basic features of animal life.⁴⁰ In December 1990 the Data Protection Registrar of the United Kingdom issued a transfer prohibition order forbidding the transfer of Personal data to the United States on the ground that US law does not provide adequate protection in the private sector.⁴¹ The issues which arise when the court considers whether interferences with expression are necessary in a democratic society can conveniently be considered under the heading of each of the ‘legitimate aims’ set out in

³⁶ Flaherty, D.H.(1984), *Privacy and Data Protection : An International Bibliography*, London: Mansell.

³⁷ *Global Privacy Protection- The First Generation-* by James B.Rule and Graham GreenLeaf- Edward Elgar Publishing Limited-UK-2008-pg.16.

³⁸ Guidelines concerning computerized personal Data Files (Doc E/CN.4/1990/72, 20 February 1990)

³⁹ UN General Assembly Resolution 2450 of 19 December 1968 (Doc E/ CN.4/ 1025).

⁴⁰ *Privacy And Human Rights- An International And Comparative Study With Special Reference To Developments In Information Technology* by James Michael- Dartmouth Publishing Company Limited, England-1994- pg.3, para 3.

⁴¹ *Whose File Is It Anyway?’ Solicitors Journal*, 15 March 1991, Vol.135, No.10, pp.304-5.

Article 10(2) of European Convention on Human Rights.⁴² Article 14 of the Constitution of Pakistan provide for dignity of man. Privacy of home and right against tortures. It was held:- “The inviolability of privacy is directly linked with the dignity of man. If a man is to preserve his dignity, if he has to live with honour & reputation, his privacy whether in house or outside the house has to be saved from invasion and protected from illegal intrusion.”⁴³ Right to life is the most fundamental of all human rights, and any decision affecting human life, or which may put an individual’s life at risk, must call for the most anxious scrutiny.⁴⁴ The sanctity of human life is probably the most fundamental of the human social values. It is recognized in all civilized societies and their legal system and by the internationally recognized statements of human rights.⁴⁵ Privacy has found protection as an international human right from the outset, being included in the Universal Declaration of Human Rights (UDHR),⁴⁶ as well as the International Covenant on Civil and Political Rights (ICCPR).⁴⁷ The South African Constitutional Court recently defined privacy as the “right of a person to live his or her life as he or she pleases”.⁴⁸ The Canadian Supreme Court has defined it as “the narrow sphere of personal autonomy within which inherently private choices are made”.⁴⁹ Article 12 of the UDHR states: No one 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 the protection of the law against such interference or attacks. The right was given formal legal protection in Article 17 of the ICCPR, which states: (1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. (2) Everyone has the right to the protection of the law against such interference or attacks. Protections for privacy are also found in the American Convention on Human Rights (ACHR) at Article 11. The relevant provisions of the ACHR state: No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his

⁴² PRIVACY AND FREEDOM OF EXPRESSION- by Richard Clayton QC and Hugh Tomlinson QC, OXFORD UNIVERSITY PRESS- 2nd edition, 2010, pg. 305, para 3.

⁴³ *Benezir Bhutto v. President of Pakistan* PLD 1998 SC 388.

⁴⁴ *Bugdaycay v. Secretary of State*, (1987) 1 All ER 940.

⁴⁵ *R(Pretty) v. DPP*, (2002) 1 All ER 1.

⁴⁶ UN General Assembly Resolution 217A(III), 10 December 1948.

⁴⁷ Adopted by UN General Assembly Resolution 2200A (XXI), 16 December 1966, entered into force 23 March 1976.

⁴⁸ *NM and Others v. Smith and Others*, 2007(7) BCLR 751, para. 33.

⁴⁹ *Godbout v. Longueuil (City)* [1997] 3 SCR 844, para. 97.

correspondence, or of unlawful attacks on his honor or reputation. Everyone has the right to the protection of the law against such interference or attacks. Article 8 of the ECHR formulates the right, as follows: Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

SUGGESTIONS

(i) The Supreme Court has included Right to Privacy in the Right to Life under Article 21. It is, therefore, proposed that a new article, namely Article 21B should be inserted on the following

21B. (1) Every person has a right to respect for his private and family life, his home and his correspondence.

(2) Nothing in clause (1) shall prevent the state from making any law imposing reasonable restrictions on the exercise of the right conferred by clause (1), in the interests of security of the state, public safety or for the prevention of disorder or crime, or for the prevention of health or morals, or for the protection of the rights and freedoms of others.

(ii) The authority should not place all the aggregated data for public to access under RTI.

(iii) There should be balance between 'privacy and purpose' when it comes to the information it collects on residents.

(iv) The online authentication, where agencies can compare demographic and biometric information of the resident with the record stored in the central database should be properly regulated.

(v) As per this data analysis for UIDAI / Aadhaar Card is used by the government for the different subsidy related food, LPG, Health, and Education etc. But it should not be made a compulsory document to avail benefits of government schemes.

(vi) The iris and retina scanned data should be protected properly, because it is capable to extract medical information of a person which violates right to privacy.

CONCLUSION

The Aadhaar Card is not only identity card but it is used by the government as wellbeing tool to provide the subsidy. A right to restrict the use of 'personal' or 'private' information about an individual is central to the right to privacy. A large volume of such information is held by public bodies and is, potentially, open to misuse. The extent to which the use of this information is controlled or restricted is one of the most important 'privacy' issues. No doubt right to life including right to privacy. And right to privacy is a fundamental right though not an absolute right.

REFERENCE

- 1) L.S. Strickland and L.E. Hunt, Technology, security, and individual privacy: new tools, new threats, and new public perceptions, *Journal of the American Society for Information Science and Technology* 56 (2004) 221–34
- 2) Miller, A.R (1971), *Assault on Privacy: Computers, Data Banks and Dossiers*, Ann Arbor, Mich : University of Michigan Press, p.40.
- 3) 1 CANNATACI, J.A., *THE INDIVIDUAL AND PRIVACY* (Routledge 2015)
- 4) J. L. MILLS, *THE LOST RIGHT* 4 (Oxford University Press 2008)
- 5) Jed Rubenfield, *The Right to Privacy*, 102 HARV. L. REV. 737, 740 (1989)
- 6) MANNHEIM, KARL & JOHN STEPHEN EROS, ED., *AN INTRODUCTION TO THE STUDY OF SOCIETY BY KARL MANNHEIM* (Literary Licensing, LLC 2013)
- 7) 2 BASU, DURGA DAS, *COMMENTARY ON THE CONSTITUTION OF INDIA* 4772 (3rd ed. Lexis Nexis 2016)
- 8) GREAT BRITAIN AND DAVID CALCUTT, *THE CALCUTT REPORT OF THE COMMITTEE ON PRIVACY AND RELATED MATTERS* 7 (Stationery Office Books 1970).
- 9) K.S. Puttaswamy v. Union of India, [\(2017\) 10 SCC 1](#)

- 10) For a discussion on the importance of computing to modern states and societies see Robertson, D.S. (1998) *The New Renaissance: Computers and the Next Level of Civilization*. Oxford University Press, United States of America
- 11) Scott, J.C. (1998) *Seeing like a state : how certain schemes to improve the human condition have failed*. New Haven: Yale University Press.
- 12) Gates, J., & Privacy Working Group. (1995). *Privacy and the National Information Infrastructure: Principles for Providing and using Personal Information*. Information Policy Committee, Information Infrastructure Task Force. Retrieved from <http://aspe.hhs.gov/datacncl/niiprivp.htm>.
- 13) G.Gurunadha Reddy v. A.P.Road Transport Corporation, AIR 1999 AP 179.
- 14) Kartar Singh v.State of Punjab (1994) 3 SCC 569.
- 15) Kharak Singh v. State of U.P., AIR 1963 SC 1295: (1964) 1 SCR 332.
- 16) District Registrar and Collector, Hyderabad v. Canara Bank, AIR 2005 SC 186 : (2005) 1 SCC 496.
- 17) (1950) SCR 88.
- 18) People's union of civil liberties v. Union of India AIR 1997 SC 568 : (1997)1 SCC 301; Sunil Batra v. Delhi Administration AIR 1980 SC 1579 : (1980) 3 SCC 488; Valsamma Paul v. Cochin University (1996) 3 SCC 545.
- 19) Kharak Singh v. State of U.P., (1964) 1 SCR 332: AIR 1963 SC 1295.
- 20) Gobind v. State of M.P., (1975) 2 SCC 148 : AIR 1975 SC 1378 : (1975) 3 SCR 946
- 21) (1994) 6 SCC 632 : AIR 1995 SC 264.
- 22) R. v. Broadcasting Standards Commission, (2000) 3 All ER 898.
- 23) (1950) SCR 88.
- 24) Sen's classic *The Idea of Justice* (Penguin Books, 2009)
- 25) Sen's writings in *The Country of Young Boys* (Oxford University Press, 2015)
- 26) K.S. Puttaswamy v. Union of India, (2018) 4 SCC 651

- 27) Westin: R wacks, The Protection of Privacy (Sweet & Maxwell, 1980).
- 28) B. Miller, "Everything you need to know about automated biometric identification," Security Technol. Design, Apr. 1997.
- 29) Smith v. Maryland, 442 U.S. 735 (1979)
- 30) P. Mell, "Seeking shade in a land of perpetual sunlight: Privacy as property in the electronic wilderness," Berkeley Technol. Law J., vol. 11, p. 1, 1997
- 31) D. Mintie, "Report from Connecticut," Biometrics in Human Services User Group Newsletter, Mar. 1997
- 32) Bowen v. Ray, 476 U.S. 693 (1986).
- 33) Westin, A.F., Privacy and Freedom, p.350, Newyork: Atheneum (1967); London : Bodley Head (1970).
- 34) Flaherty, D.H.(1984), Privacy and Data Protection : An International Bibliography, London: Mansell.
- 35) Global Privacy Protection- The First Generation- by James B.Rule and Graham GreenLeaf- Edward Elgar Publishing Limited-UK-2008-pg.16.
- 36) Guidelines concerning computerized personal Data Files (Doc E/CN.4/1990/72, 20 February 1990)
- 37) UN General Assembly Resolution 2450 of 19 December 1968 (Doc E/ CN.4/ 1025).
- 38) Privacy And Human Rights- An International And Comparative Study With Special Reference To Developments In Information Technology by James Michael- Dartmouth Publishing Company Limited, England-1994- pg.3, para 3.
- 39) Whose File Is It Anyway?' Solicitors Journal, 15 March 1991, Vol.135, No.10, pp.304-5.
- 40) PRIVACY AND FREEDOM OF EXPRESSION- by Richard Clayton QC and Hugh Tomlinson QC, OXFORD UNIVERSITY PRESS- 2nd edition, 2010, pg. 305, para 3.
- 41) Benezir Bhutto v. President of Pakistan PLD 1998 SC 388.

- 42) *Bugdaycay v. Secretary of State*, (1987) 1 All ER 940.
- 43) *R(Pretty) v. DPP*, (2002) 1 All ER 1.
- 44) UN General Assembly Resolution 217A(III), 10 December 1948.
- 45) Adopted by UN General Assembly Resolution 2200A (XXI), 16 December 1966, entered into force 23 March 1976.
- 46) *NM and Others v. Smith and Others*, 2007(7) BCLR 751, para. 33.
- 47) *Godbout v. Longueuil (City)* [1997] 3 SCR 844, para. 97.
- 48) Dr.Lakshmi T and Rajeshkumar S “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, March 2018.
- 49) Trishala A , Lakshmi T and Rajeshkumar S,“ 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, April 2018.

