Privacy Issues of Smart Cities: Legal Outlook

Shambhu Prasad Chakrabarty, Jayanta Ghosh, and Souvik Mukherjee

Abstract The biggest consumers of technology in recent decades are the urban and semi-urban populace, especially in the developing economies. This integration of humans and technology has unravelled novel challenges in protecting various socio-economic rights of the people, enshrined in the United Nations Sustainable Development Goals (UNSDG). This paper tends to unravel the truth behind such promises in the Indian context, in her endeavour to bridge the digital divide in the internet of things. The paper focuses upon the current position of privacy laws in India and makes a contrast with leading democracies to unearth the challenges; technology would have to address in the coming decades. The debate involved in 'realization and recognition' coupled with enforcement mechanisms adopted in India would be integrated with this paper to clarify the need for protecting data privacy towards a sustainable and smart city.

Keywords Data privacy and smart cities · Smart cities and data protection laws · Smart cities and UNSDGs · Privacy rights · Data protection laws

1 Introduction

One of the severe challenges that we face today is the rise in human population leading to an imbalance in resource management. Almost half of the world population live in the existing cities causing an extension of city jurisdiction into semi-urban areas. This

S. P. Chakrabarty (✉) · J. Ghosh · S. Mukherjee
Centre for Regulatory Studies, Governance and Public Policy, The West Bengal National University of Juridical Sciences, Kolkata, India
e-mail: spc@nujs.edu

J. Ghosh
e-mail: jayanta.crsgpp@nujs.edu

S. Mukherjee
e-mail: souvik.crsgpp@nujs.edu

C. Chakraborty et al. (eds.), *Data-Driven Mining, Learning and Analytics for Secured Smart Cities*, Advanced Sciences and Technologies for Security Applications, https://doi.org/10.1007/978-3-030-72139-8_14

has created a worldwide demand for planned cities with optimum resource management. Technological advancements have further assisted this endeavour giving light to the concept of smart cities. Limitless efforts by all stakeholders made this dream come true as we witness many smart cities functioning precisely as was dreamt of. The adaptability of electronics which are inherent in smart cities, is however not compatible with the existing laws of the land. Smart city projects in developing jurisdictions like India are equally plagued with various legal challenges. The conservative and rights activists have raised serious concerns over these inherent challenges which requires proper answers. Questions of surveillance, infringement of privacy have moulded public opinion against governments promoting smart cities. In light of these challenges, it is important to identify the right course of action that is required to be adopted to make smart cities a reality.

This paper focuses on the relevance of privacy laws in the era of the IoT by exploring privacy laws prevailing in some major jurisdictions. Smart cities are connected on the web in a more intrinsic way where the inherent right to privacy becomes vulnerable and subject to compromise. The paper is divided into six parts with the first describing the concept of privacy and confidentiality. The second part highlights the collective legal position on privacy and data protection. The third studies the concern relating to 'Realization and Recognition' and the debates revolving around them. The fourth part explores the various enforcement mechanisms protecting the privacy right of the people. The fifth part elucidates the concept of smart cities and its impact on the law while the sixth explains the challenges and future direction. The paper concludes with a set of suggestions to bridge the dichotomy that exists between privacy laws and smart cities of this millennium (Fig. 1).

The major contribution of this chapter is as follows:

- It reviews Data Privacy laws
- It reviews the legal position of right to privacy and the various data protection laws prevailing in multiple jurisdictions. It also highlights the multiple legal challenges that the technology needs to adapt to be effectively acceptable.

The methodology required to be adopted to justify the objectives of the chapter is doctrinal. The researchers adequately explored the various dimensions of the method. They identified the existing legal positions on data privacy and challenges thereto, that 'smart city projects technologies' need to address to become viable in developing economies.

IoT would face immeasurable socio-political pressure in the next few decades unless they comply with the identified aspects reflected in this chapter.

2 Understanding Privacy Rights

One of the major challenges against smart city movement is privacy. To unravel the concept of privacy, it is essential to understand that it is an integral part of a much broader, though, called rights. Rights of an individual emancipated from the

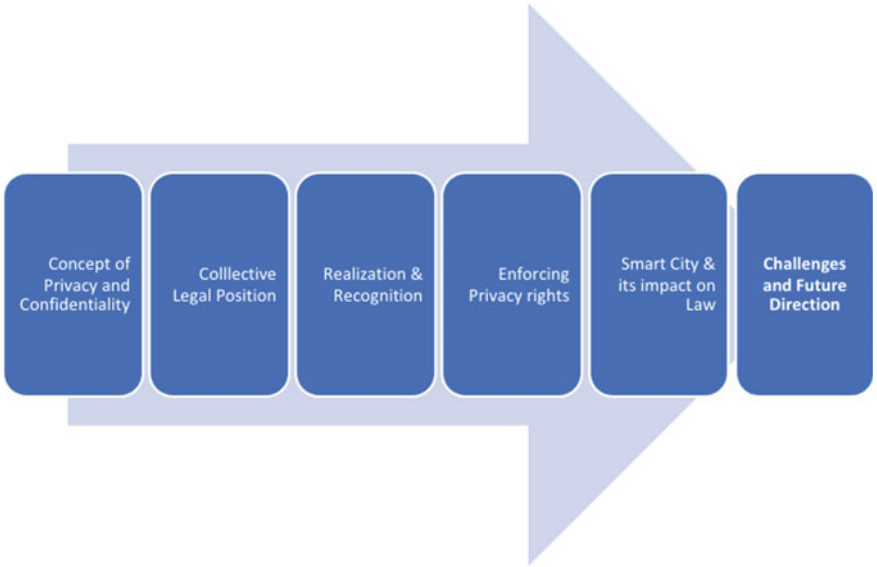

Fig. 1 Structure of the chapter

growth of liberty, which was a struggle of centuries. Magna Carta is considered to be the first document depicting rights as inherent in man and not dependable upon the whims of the king or the sovereign. Right to privacy evolved overtime and flourished in common law jurisdictions mainly in Europe and the west. Post-WW-II, in the decolonization era, human right evolved as an integral part of rights fundamental to human existence. Various new constitutions, including that of India, recognized privacy right as a justiciable right.

Raymond Williams traced the etymology of the word private to its Latin privatus, implying "withdrawn from public life", or "to bereave or deprive" [1]. From the sixteenth to nineteenth century, the word privacy has acquired a "sense of secrecy and concealment" [1]. It has also very significantly transitioned to denote the "conventional opposition to the public like a private house, private education," and "private property," all of which represented the "primary sense of privilege [where] the limited access or participation was seen not as deprivation but as an advantage" [1].

To equate privacy as an inherent and a fundamental right, it is necessary to look into the origins and growth of the concept of privacy [2]. This development of the concept of privacy can notably be dependent on several international instruments including the great Magna Carta [3]. More recent instruments like "Universal Declaration of Human Rights" (UDHR) [4], "International Covenant on Civil and Political Rights" (ICCPR) [5], "Convention on the Rights of the Child" (CRC) [6], "International Convention on the Protection of All Migrant Workers and Members of Their Families" (ICPAMWF) [7], the "European Convention on Human Rights" (ECHR's) [8] or the "American Convention on Human Rights" (ACHR's) [9] have acknowledged 'privacy right' in one form or the other. In recent decades, with the advent of

internet, a strong relationship could be found between privacy and data protection [9]. Discussions have started making rounds with the use of cameras (surveillance) and debate of reasonable use of computers in the society where personal data of every specific individual is collected and also stored [10].

Privacy as a right was recognized by the UDHR and other major international instruments which provoked major jurisdictions to incorporate it as a right which is fundamental [11].

3 Collective Legal Position on Privacy and Data Protection

'Information' is considered as the 'greatest wealth' in the modern era, the statement is truer than ever in the era of internet and Big Data. Data, which is received, collected and stored, is generated from the society and converted into information which is used 'for' or 'against' its generating source i.e., the people, the society, the mankind. The concerns regarding the privacy of data are multifaceted as it impacts all aspects of life. These concerns are attacked by several forms of acts including, but not limited to, cyber-frauds, cybersecurity breach, etc. A substantial development has been witnessed in the process of law-making in this area of discourse, internationally. Needless to say, that this would require international law to play a significant role as well. However, there remains a void in this area in terms of common regulation addressing the specific issue of data privacy, rather the international conventions, treaties, declarations on human rights and regional instruments have shaped the development of regulation across the world.

One of the earliest international instruments which addressed the concerns of privacy of individuals was the "Universal Declaration of Human Rights", recognising individuals' privacy and dignity [4]. The document was inspired by the horrors of the Second World War, as the world extensively witnessed the realisation of a potential threat from the State machinery. Article 12 of the UDHR prohibits "*arbitrary interference*" in the privacy and dignity of individuals and their families [4]. Individual's privacy concerns were reiterated in Article 17 in 1966 in the "International Covenant on Civil and Political Rights" [5]. "The Convention for the Protection of Human Rights and Fundamental Freedom," popularly known as "European Convention on Human Rights," also respects the privacy of every individual; with an exception to the issues and concerns of public safety, national security, the economic well-being of the state, crime prevention, protection of health or the moral state or rights and freedom of others demand such interference; albeit such intervention should be done in accordance with the law [12]. The initial developments in the concerns of privacy were protection of individual piracy from arbitrary interference of States.

3.1 Collective Initiative—European Union

As the technology advanced, the vulnerability of an individual's privacy increased by leaps and bound, and it was no more the concerns of arbitrary intervention by State machinery but from non-State actors too. To address the ever-growing challenges to protect and respect individual's privacy and related concerns, the European nations took several affirmative steps collectively, which are as follows:

(A) ***Convention 108***

The technological advancement inspired the European nations "to address the issue of protection of data privacy as a collective". The member nations of the European Council, with a view of protecting fundamental rights, especially the right to privacy and a significant rise in automated personal data processing ("data protection"), came up with the "Convention for Protection of Individuals concerning Automatic Processing of Personal Data, 1981" also known as "Convention 108" [13]. As per the Convention,

> The automatic processing meant storage of data, carrying out of logical and/or arithmetic operation on those data, alteration, erasure, retrieval or dissemination [13].

It fell upon the member States to make such legislation governing the privacy rooted in the fundamental principles of the Convention. The Convention obligated the nation-States parties to prohibit automatic processing of data relating to race, political or religious belief, health and sexual life unless domestic laws are enacted with safeguards. Guidelines are related to additional safeguards which rectify or erase such data which are obtained or processed by violating or ignoring the domestic legislations. Furthermore, a specific exception was made to the basic principles for the protection of data reflecting similar provisions as provided in the "European Treaty on Human Rights" [12]. Following the Convention 108, in 1995, the European Parliament issued a directive addressing personal data processing and its free movement [14]. The objective of the directive was to protect the right to privacy of personal data and allied processes involved in handling such data [14]. Personal data is to be interpreted as information related to a natural person, irrespective of the way or method it is acquired, directly or indirectly. These data may include information relating to the physical, mental or physiological features as well as the social, economic or cultural characteristics of an individual [14]. Thereafter concerning the health and medical data protection several collective measures were taken by the European Council such as Oviedo Convention, Declarations on Promotion of Patients' Rights in Europe, Opinion of the "European Group on Ethics in Science and New Technologies," however, the 1995 Directives on Data Protection were governing the processing and free movement of data until 2018.

(B) ***Regulation on General Data Protection by European Parliament***

The introduction of AI and big data changed the dynamics of data collection and information processing significantly. Not surprisingly, data protection became more

challenging. The Consultative Committee of the Convention prescribed guidelines for the protection of automated data privacy rights, the guideline included human rights, fundamental freedoms and necessity for compliance with data protection. The far-reaching and penetrative impact of big data was recognised and the related privacy concerns as raised in Convention 108 were reiterated in the wake of the potential implications of big data processing and artificial intelligence. These guidelines through specific clauses limited the unauthorised use of various personal data.

In 2018, the "European Parliament and Council of European Council" implemented "Regulation (EU) 2016/679," which deals with privacy and data protection of the European Union [15]. The regulation is known as "General Data Protection Regulation (hereinafter referred as GDPR)," it repealed the earlier Directive 95/46/EC and considered one of most comprehensive documents addressing the concerns of data protection and privacy in the contemporary time. The GDPR has a far-reaching effect, as even though it is a creation of European Union, it imposes an obligation on the organisations engaging in the collection of data, from people in the European Union, irrespective of the location of the organization [16]. The Regulation entails hefty penalty upon the violators of the standards relating to privacy and security as laid down by the regulation. The regulation is premised upon the principles of transparency, fairness and lawfulness, purpose limitation and limiting data collection; the accuracy of data; temporal limitations on storage; integrity and confidentiality and accountability [15]. The regulation is divided into eleven chapters, wherein it explicitly addresses "the concerns of rights of the subjects, obligations of controllers and processors, data security and protection, code of conduct and certifications, provisions relating to transfer of data to third countries or international organisations, independent supervisory authorities, provisions addressing the co-operation, coordination, remedies, liabilities, penalties etc." [15].

Irrespective of the applicability of these regulations on the member countries of the EU, the Even though the regulation at present is applicable amongst the EU members, the standards are nonetheless acceptable in countries outside the EU. It can be argued that the said standards would play an important role in shaping up of international data protection law on healthcare. Furthermore, this trend of accepting the standards of nations other than European countries may lead to the creation of customary international law, albeit with specific modifications, exceptions and reservations, and successfully remove the void in international law in the area.

Inspired by the initiatives taken by the European Union, several nations have developed laws on data protection or on the path of creating such laws, an indicative Table 1 is given hereunder.

4 Realization and Recognition—Debate

Absence of a global law on privacy and data protection can be felt in almost all complications arising from cases where transactions involved multiple countries. The technological solutions to address the challenges of a modern economy have

Table 1 Indicating privacy and data protection laws in selected countries

Country	Laws	Features
USA	HIPPA	Right to privacy for every individual from 12 years through 18 years "Individuals violating the confidentiality provisions are subjected to a civil penalty"
UK	DPA	Individuals are provided with ways to control information Prohibition of data transfer to other jurisdictions excluding the EEA
EU	Data Protection Directive	Protects the people's "right to privacy including the processing of personal data" [17]
Russia	"Russian Federal Law on Data Protection"	Creates an obligation over the data operators regarding the "protection of personal data against unlawful or accidental access"
India	IT Act	Reasonable data protection practices including civil and penal provisions in case of violation [18]
Canada	PIPEDA	"Individuals have the right to know the reasons for the collection of data. Organisations dealing with data are required to protect such information" [19]
Brazil	Constitution	"The intimacy, private life, honour, image of the people including assured rights to indigenization by material or moral damage resulting from its violation" [20]
Morocco	The 09-08 Act	"Protects the one's privacy through the establishment of the CNDP authority by limiting the use of personal and sensitive data using the data controllers in any data processing operation" [21]
Angola	"Data Protection Law no. 22/11 of 17 June"	"Concerning the sensitive data processing, collecting and processing is only allowed where there is a legal authorisation from APD" [20]
Bangladesh	Digital Security Act, 2018	Section 26 guarantees the need for explicit consent of individuals for collecting, selling, storing or preserving personal information
Pakistan	No specific Law (Personal Data Protection Bill is there)	Certain requirements and restrictions in "processing of personal data" have been proposed in the Bill
Nepal	No specific Law	Section 28(2) of "The Right to Information Act, 2007" has tried to address this legal vacuum
Kenya	Data Protection Act, 2019	Comprehensive laws to protect the personal information of individuals

(continued)

Table 1 (continued)

Country	Laws	Features
Australia	The Privacy Act 1988	It promotes and protects the privacy rights of individuals and regulates state agencies and some other organisations

raised debates and at times left a very delicate position to ponder upon. The search of a simplified response to this dynamic nature of IoT has led to a surreal of questions from various corners [3]. One such question "*if you have nothing to hide, then what do you have to fear*?" has been going around for quite some time. Contrary to this view, "*if you aren't doing anything wrong, then what do you have to hide?*" arguments have put been raised to counter the former. This dichotomy unfortunately does prevail with any specific answer to settle the debate. According to Judge Richard Posner, "*When people today decry the lack of privacy, what they want, I think, is mainly something quite different from seclusion/privacy; they want more power to conceal information about themselves that others might use to their disadvantage.*" Privacy includes a person's "*right to conceal discreditable facts about himself*" [22]. Again Charles Fried noted that privacy is one of the basic *rights in rem*, rights to which all are entitled equally, by virtue of them as persons [3] cannot be undermined. The arguments raised on either side have brought up some cardinal human nature which is required to be realised and also recognize amidst the debate.

McWhirter, argued that, "Democracy assumes political equality, but that is difficult when there is economic inequality, a necessary consequence of the free enterprise system. Democracy assumes rule by the majority, but what if the majority wants to interfere with the liberty of a minority? This in turn raises the question: What areas should be left to the conscience of the individual citizen and what areas are legitimate subjects of legislation? Put another way: Where do democracy end and liberty begin?".

Now in interpreting 'what is the right of privacy?' from the above observations made, a discussion of Judge Cooley seems relatively relevant. In his classical work on Torts, he recognizes "right to be let alone" as one of the inherent rights of any human being [3]. This is further supported by John Gilmer Speed who emphasized that, "*as the man comes into the world alone, goes out of it alone, and is alone accountable for his life, so may he be presumed to have by the law of his nature full right to live alone when, to what extent, and as long as he pleases*" [23]. Thus the question of privacy as a right has been admired and accepted in almost all jurisdictions today in the world. However, with the complications of the modern digital world, "absolute expectations of privacy" have given way to "reasonable expectation of privacy".

Austin herself has claimed that the notion of a "reasonable expectation to privacy" is itself an attempt to balance the individual's right to privacy with other competing interests, but that such an approach can be viewed in one of the three different contexts. First, a reasonable expectation can refer to an attempt to balance the individual's privacy interest against the state's need to limit that privacy to advance the state's interests, where the balance sought is defined by the outcome of such

balancing [24]. A second context of the balance sought is in the reasonable expectation that relates directly to the appropriateness or legitimacy of the privacy claim itself because of social norms or conventional expectations [24]. Third, the notion of finding a balance between the individual and society is ignored and "an individual's privacy interest is defined in light of society's interests rather than balanced against these interests" [24].

Deckle McLean identified "four basic types of privacy" viz., access control; room to grow safety-valve; and "respect for the individual," [25], which is required to be addressed in the new millennium amidst the growth of IoT [26] on one hand and the responsibility to attain the UNSDGs on the other.

5 Smart Cities

Irrespective of a diversified nomenclature, the concept underlying smart cities (technology-infused cities) [27–30] revolve around six cardinal aspects, economy, governance, people, living, environment and mobility. However, there are many other analogous and distinctive aspects of the concept of smart cities. These aspects revolve around a few objectives including, employment opportunities, investment opportunities, economic activities which ultimately improve the quality and standard of life. Consequently, people shall live a more comfortable and sustainable life with optimum happiness who would live in these cities.

Smart cities would arguably provide technical solutions to existing challenges faced by the over-populated urban populace. As the world moves towards urbanisation and having half of the population living in cities, the challenges are time tested and require technical solutions without a doubt. To make things complicated, a recent study reveals that by 2050, two-third of the world's population would shift to an urban environment. The natural tendency of people moving towards an environment with opportunities for a better and comfortable life has made further complication to the existing cities. These unsolved challenges have put the onus of the governments to plan a city life accommodating various essential services un-affected and undisturbed. For example, city administration, cost-effective power, fuel and water consumption, citizen involvement in public services. The expectations are high, especially from smart cities, as it is expected that, "cities [will] deliver where nation-states have failed" [31].

6 Impact of Smart Cities

The impact of smart city projects has shown very promising results [32]. The economic growth of the people has been one of the promising impacts of smart city initiatives. The service industry has seen significant growth with specialists getting

jobs for various automation services and maintenance. The domination of computer science, engineering and networking, has been witnessed in some studies.

It is during 1990s pure technological theories were started to be tested with various social and cultural implications. Even political and economic parameters were also tested upon the STEM-driven smart city models. This new dimension of research unravelled a few social critiques of Smart cities [33] as classified hereunder leading to political turmoil and at times ousting of the political party in power democratically during elections by a considerable margin, leading to an abrupt halt, in developing a smart city.

6.1 Overemphasis on Technical Solutions

Technological solutions are based on the presumption that everyone has a specific problem in hand, and they look for a solution which can be crafted uni-dimensionally. The example of locating a place through GPS is a fit case to illustrate this position. This, unfortunately, does not hold good where structural solutions are required over technological solutions, like that of the pressing challenge of climate change or change in the population patter from homogenous to heterogeneous. Technological marvel has in most cases outshined the reality of our society which demands a heterogeneous over homogenous solutions to their distinctive challenges. Again, technological developments have largely been an outcome of commercial investments which ultimately objects to maximisation of profit for the originating or the host institution which provides service thereof. Large socio-economic challenges can also be met by the application of technology, which unfortunately is missing amongst the front running developers.

6.2 Top-Down Implementation and Technocratic Governance

The role of citizens in any city must be primary as opposed to the position in smart cities where initiatives are driven by corporate-government bureaucracies as opposed to democratic governance. Smart cities need to be smart enough to accommodate people from every sector there is to live life to their potential. Unfortunately, the digital divide is more economic than social, due to the top-down implementation and technocratic governance.

6.3 Corporatization and Privatization

There has been an increasing number of functions and roles being delegated by the government upon the private players because these actors have created these smart

cities and are perfectly placed to provide such services. This delegation of power is not merely a service contract but a smart opportunity for the profit-seeking private actors to work to that end. Smart cities have unfortunately shown to promote corporatization and privatization of public spaces where economic disparity exists. This predominantly benefits the rich elites, compromising the welfare of large portions of the city with an economically weaker population.

6.4 Reinforcing Divides and Inequities

City life includes within its domain a heterogeneous populace where there is inequality, poverty and marginalization. The existence of these elements and models of smart cities including these parameters are recently explored [34]. Unless the smart city accommodates within its fold, the most vulnerable and marginalised, the digital divide would only be encouraged and only the economically able be accommodated within the fold of smart cities, which is an impractical proposition in developing economies.

6.5 Surveillance and Privacy Violations

Smart cities not only suffer from these fatal flaws but also hand over a significant number of public functions including surveillance and law enforcement on private actors. Private enterprises, needless to say, focus upon profits over the greater good, as is the duty and responsibility of the state over its subjects in their governance. This paper primarily focuses on Surveillance and Privacy violations coupled with the laws and regulations prevailing in India in this regard.

6.6 Security Concerns

Discrimination, marginalisation and inequality which exist in our society could be multiplied in smart cities where everyone is under surveillance. Smart methods of surveillance, like geo-tracking and profiling, pose a great threat to the privacy of an individual which could be averted in a world of non-digital surveillance. Smart cities are equipped with hundreds of interconnected gadgets which communicate and distribute data amongst themselves. This modern technological marvel posing privacy threats cannot be ignored as identification of data is swift and clear in case the party in power so desire to identify and shun the voice of opposition in a democracy. Needless to say, the easy availability of many private data like religious or political orientation would additionally provide many implications on governance, exposing individuals to harm's way. Thus, contrary to the notion of developing neutrality on

governance, modern and future governance can be plagued with radical profiling through machine learning and the internet of things. These technologies would naturally be used to suppress any form of political dissent. As rightly reflected, "a person's data shadow does more than following them; it precedes them" [35], creating far-reaching effect to the life and liberty of citizens living in smart cities.

6.7 How Privacy and Security Are Two Distinctive Concerns?

Security in the first place provides the "ability to be confident" regarding the fact that decisions being taken by individuals are respected. On the other hand, "privacy is the ability to decide what information of an individual are provided and what are not" and also includes where it goes.

Consent plays a pivotal role in the case of private and sensitive information of an individual. In other words, the data cannot be transferred without the prior consent of the individual. On the other hand, various things like firewall, encryptions etc., are used to prevent tampering of security systems to unauthorized access and use of data by third parties.

Privacy creates an obligation on the part of the agency in possession of data to identify appropriate use of such data. Security, on the other hand, is the "confidentiality, integrity and availability" of such data [20].

6.8 Consent in the Digital World! Is It Informed Consent?

Consent is given when there is consensus ad idem (thinking on the same thing in the same sense) by the parties. In the digital era, the contracting parties are in no uniform thinking platform, on which they agree. The manufacturer of a cell phone for example has a much-sophisticated knowledge over the device than the consumer. The buyer of the cell phone also does not have any idea at the time of purchase that they have to agree to a plethora of clauses protected by an agreement which they would have to consent to use the said devise. Subsequently, the customer or the user, do not have any knowledge or idea as to where the said devise is automatically connecting and sharing his personal and professional data and information. The point of no return is when the huge amount has already been paid by the customer before activating the device. Once the said devise is purchased, the customer would not practically use a one lakh rupees cell phone as a paperweight and would use the cell phone as intended irrespective of the intention of not accepting the terms and conditions. Thus, the state must introduce a policy of basic use platform which would not infringe various privacy issues of the users.

Another illustration of this dilution of consent can be noticed from the growing use of health monitoring devises manufactured by fit bit, apple, Samsung etc. The consumers are not even aware of the web their health care data is transmitted on a

minute-to-minute basis. The consumers were neither informed by these manufacturers nor are they aware of the threats that these devices may bring to them. The devices are connected in such a way that they would not work independently but start connecting and communicating to multiple devices without informing the user [36]. There is no mode available in these devices which would make them work independently outside networks. The data generated from these millions of demises ultimately helps AI to play its part in the life and liberty of the consumers. A study revealed that the monitoring of water meters can unveil whether a person is bathing in the house at a given time [36].

Broadly, these technology-driven devices are intended to accommodate surveillance and infringement of privacy of an individual at any given time in a smart city where everything is based on surveillance. Do the end-users consent to all these violations at the time they purchased these gadgets like handheld or wearable devices?

6.9 Internet of Things and Data Privacy

IoT is a global architecture based on the World Wide Web (www) which facilitates the exchange of services as well as goods [37]. It plays a major role within the supply chain network globally [37]. As a natural consequence, IoT impacts the privacy and security issue of various stakeholders [37]. Strategic safeguards which ensure the architecture's resilience in case of a security breach, authentication of data, to control the access of confidential information and client privacy are required to be established [38]. Amidst the technological functioning, the regulatory mechanism needs to be established both from the global and local jurisdictions. Irrespective of the dynamic nature of the challenge, it is very much possible to initiate a mechanism to make regulatory determinations at the global level with private players adapting to such requirements [38]. The viability of this mechanism shall largely depend upon the global acceptance of a similar standard of the right to privacy and data privacy.

As discussed earlier, both privacy and security are issues of great concern of the public. Having a comprehensive guaranteed solution to the issue of security and privacy would be welcomed facilitating widespread adoption of IoT.

Historically, the concern of privacy and security of personal data was not a necessity. However, with time, the importance of protection of data and personal information became clear for the success of IoT. Technical experts could manage, somehow, to develop ways to secure and protect private information, but they looked like mere patchworks. Significant flaws could be identified in the process and no security could be said to be a guaranteed and full proof system to protect data. Public acceptability for the IoT will only be a reality when satisfactory security and privacy solutions would be available. In practice, taking security and privacy challenges from a technical perspective would not provide an adequate solution unless the issues are considered from socio-ethical considerations [39].

7 Challenges and Future Direction

Smart cities are very important as they provide the opportunity to solve many challenges un-addressable till now including the potentiality to achieve UNSDGs at one go. In other words, smart cities look like a reality coming out of the fiction novels. And this has been possible due to the enormous development of technology. Irrespective of the potential benefits of smart cities, city life must be trustworthy to the city dwellers when it comes to privacy and security. The wrong side of technology has always haunted the people including that of policy makers, reminding them the danger that looms large upon them, if the control is intercepted by whims and arbitrariness.

With the world moving under the global umbrella of technology, there is no such thing as a global data protection law. Even when UDHR, OCED Privacy Principles [40] and other similar instruments have assisted in making privacy a right which cannot be abrogated, there is a vacuum when it comes to a global data protection law. Even when major countries have their laws of data protection and privacy, there is a significant variation amongst themselves and in some cases, confliction provisions on the same issues can also be noticed. With the IoT and transactions beyond boundaries, identifying specific laws to comply in cases of distributed digital activities has always been a challenge. Cross border transfer of data, for example between the EU and US, has been a high voltage drama to look at in recent years. Measures like "safe harbour" [41] and more recently "privacy shield" [42] to mitigate the complexity of the situation has been adopted.

The smart city must adapt its technology with the existing regulations on one hand and must be in a position to adjust with future regulations, to be a success story in the decades to come. This can be achieved with a strategic and systematic change in the way smart city policy is framed. Precedents of success stories in other countries would not hold good in many complex societies like that of ours. Thrust must be given to make the smart city accommodate every section of the society. Technology must now be used to tackle social challenges like education, health etc. to make it acceptable to all sections of the society. Technology must accommodate necessary protection against political surveillance and victimisation of critics. Right to be forgotten must be protected, technologically, with very limited exceptions. To imitate the successful path of smart cities like Singapore, in India would not be a romantic journey for sure, as can be witnessed with our very own Amaravati [43]. A more reasonable and balanced journey for smart cities to be successful would definitely be, to bring technology for public good, diversity, accessibility and inclusivity, to cater government to solve complicated problems, to bridge barriers and hear diverse voices.

With the advent of blockchain technology one of the key concerns for any modern society is the protection of privacy rights pertaining to healthcare data [44]. Healthcare Sector and technological innovation is one the most significant developments of the twenty-first century, hence smart cities would be apt to launch pilot projects addressing the induction of latest technological advancements adapting to the existing

and future legal mechanism to observe and determine its efficacy. Furthermore, smart cities may also facilitate pilot projects, for application of contact tracing and warning measure models with respect to emergent situations, akin to the COVID-19 pandemic, as well as application of AI [45, 46].

8 Conclusion

The paper reiterates the need of a responsible set of technologists who would take care of making a smart city live able inter alia, without fear of being in a state of constant vigilante and prosecution. Smart city projects will keep on facing similar challenges at least till the aforesaid position changes. It is advisable, under the said scenario that the scientists should start focusing on making the technology compliant to the basic laws of privacy. Failing this, which is most likely to happen, would only delay smart cities from being a reality. Bereft of legal compliance, technology would not blossom in the way it could be in the years to come. Non-compliance of domestic laws coupled with ignorance of international legal regime has brought unprecedented interruption to the growth of technology-driven systems in India, that would otherwise flourish and solve many practical and social challenges. The future of technology-driven methods would largely depend upon the jurisdiction's legal discourse. Modern developers must be compliance proof and flexible to adapt to the changing legal regime. Once we achieve this, there would be a significant reduction of unwarranted disruption invoked by litigation.

References

1. Williams R (2014) Keywords: a vocabulary of culture and society. Oxford University Press, p 203
2. Warren SD, Brandeis LD (1890) The right to privacy. 4 Harv L Rev 193
3. Commentary of The Charter of Fundamental Rights of The European Union, Article 6. Right to liberty and security, p 67. https://ec.europa.eu/justice/fundamental-rights/files/networkcommentaryfinal_en.pdf
4. Universal Declaration of Human Rights, Article 12 of the Declaration "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation". https://www.un.org/en/universal-declaration-human-rights/
5. ICCPR, Article 17(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". https://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx
6. CRC, Article 16(1), "No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation." https://www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx
7. ICPAMWF, Article 14, "No migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her privacy, family, correspondence or other communications, or to unlawful attacks on his or her honour and reputation. Each migrant

worker and member of his or her family shall have the right to the protection of the law against such interference or attacks." https://www.ohchr.org/en/professionalinterest/pages/cmw.aspx
8. ECHR's, Article 8, "Right to respect for private and family life." https://www.echr.coe.int/documents/guide_art_8_eng.pdf
9. ACHR's, Article 11. "Right to Privacy", Clause 1. "Everyone has the right to have his honor respected and his dignity recognized." https://www.cidh.oas.org/basicos/english/basic3.american%20convention.htm
10. De Leeuw K, Bergstra J (eds) (2007) The history of information security: a comprehensive handbook. Elsevier
11. UDHR, Article 12 of the Declaration "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation". https://www.un.org/en/universal-declaration-human-rights/
12. European Convention on Human Rights. https://www.echr.coe.int/documents/convention_eng.pdf
13. Convention 108. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108
14. EC Directive 95/46/EC. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046
15. Regulation (EU) 2016/679. https://gdpr.eu/what-is-gdpr/#:~:text=The%20General%20Data%20Protection%20Regulation,to%20people%20in%20the%20EU
16. GDPR. https://gdpr.eu/what-is-gdpr/#:~:text=The%20General%20Data%20Protection%20Regulation,to%20people%20in%20the%20EU
17. Craig T, Lulloff M (2011) Privacy and big data: the players, regulators and stakeholders. O'Reilly Media, Inc
18. Information Technology Act 2000, Chapter IX & XI (India). https://www.indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf
19. Jensen M (2013) Challenges of privacy protection in big data analytics. IEEE International Congress on big data
20. Abouelmehdi K, Beni-Hessane A, Khaloufi H (2018) Big healthcare data: preserving security and privacy. J Big Data 5, 1. https://doi.org/10.1186/s40537-017-0110-7
21. Data protection overview (Morocco)—Florence Chafiol-Chaumont and Anne-Laure Falkman (2013)
22. Solove DJ, Schwartz (2014) Information privacy law. Wolters Kluwer Law & Business
23. Speed JG (1896) The right of privacy. North Am Rev 163(476):64–74
24. Austin L (2003) Privacy and the question of technology. Law Philos 22:136
25. McLean D (1995) Privacy and its invasion. Praeger, Westport CT, pp 47–60
26. Sucharitha M, Chakraborty C, Rao SS, Reddy VSK (2021) Early detection of dementia disease using data mining techniques. In: Springer: Internet of things for healthcare technologies. Studies in big data, vol 73, pp 177–194. https://doi.org/10.1007/978-981-15-4112-4_9
27. Dutton WH (1987) Wired cities: shaping the future of communications. Macmillan Publishing Co., Inc
28. Graham S, Marvin S (1999) Planning cybercities? Integrating telecommunications into urban planning. Town Plan Rev 89–114
29. Ishida T, Isbister K (eds) (2000) Digital cities: technologies, experiences, and future perspectives. Springer Science & Business Media
30. Batty M (1997) The computable city. Int Plan Stud 2(2):155–173
31. Oomen BM (2016) Introduction: the promise and challenges of human rights cities. Cambridge University Press
32. OECD (2020) Smart cities and inclusive growth. https://www.oecd.org/cfe/cities/OECD_Policy_Paper_Smart_Cities_and_Inclusive_Growth.pdf
33. Dutta A (2018) The digital turn in postcolonial urbanism: smart citizenship in the making of India's 100 smart cities. Trans Inst British Geograph 43(3):405–419
34. Reuter TK (2019) Human rights and the city: including marginalised communities in urban development and smart cities. J Human Rights 18(4):382–402

35. Kitchen R, Cardullo P, Feliciantinio C (2019) Citizenship, justice and the right to the smart city. In: Cardullo P, Feliciantinio C, Kitchen R (eds) The right to the smart city. Emerald Publishing, Bingley, UK
36. Commscope, Connectivity as the fourth utility in smart cities. https://www.commscope.com/globalassets/digizuite/2340-connectivity-as-the-4th-utility-in-smart-cities-co-113342-en.pdf?r=1
37. Weber RH (2009) Internet of things—need for a new legal environment? Comput Law Secur Rev 25:521
38. Weber RH (2010) Internet of things—new security and privacy challenges. Comput Law Secur Rev 26(1):23–30
39. 3rd international conference on advanced computer theory and engineering (ICACTE—2010). https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5579543&tag=1
40. OECD privacy guidelines. https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm
41. Maru P, From safe harbour to privacy shield to GDPR: the journey of data protection laws. https://cio.economictimes.indiatimes.com/news/government-policy/from-safe-harbour-to-privacy-shield-to-gdpr-the-journey-of-data-protection-laws/64327558
42. US-EU privacy shield principles. https://www.privacyshield.gov/eu-us-framework
43. Aggarwal M, Within five years, Andhra Pradesh capital Amaravati has gone from a promised utopia to 'ghost town'. https://scroll.in/article/934122/within-five-years-andhra-pradesh-capital-amaravati-has-gone-from-a-promised-utopia-to-ghost-town
44. Chakrabarty SP, Mukherjee S, Rodricks A (2021) Data protection and privacy in healthcare: research and innovations. In: Elngar RF, Pawar A, Churi P (eds) The role of law in protecting medical data in India, 1st edn. CRC Press, pp 229–245. https://doi.org/10.1201/9781003048848 (forthcoming)
45. Garg L, Chukwu E, Nasser N, Chakraborty C, Garg G (2020) Anonymity preserving IoT-based COVID-19 and other infectious disease contact tracing model. IEEE Access 8:159402–159414
46. Chakraborty U, Banerjee A, Saha JK, Sarkar N, Chakraborty C (2021) Artificial intelligence and the fourth industrial revolution. Jenny Stanford Publishing Pte Ltd. ISBN 978–981–4800–79–2 (Hardcover), 978–1–003–00000–0 (eBook)