 DOI: *https://doij.org/10.10000/IJLSI.11882*

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 3 | Issue 4

2021

Internet of Things & Personal Data Protection: A Critical EU Law Perspective

ARUSMITA ACHARYA[1] AND BHARATH CHANDRAN P S[2]

ABSTRACT

Technology has advanced dramatically since the late twentieth century. The emergence of technology has been one of the most important technological landmarks as far as the modern day is concerned. Technology that was just limited to computers has progressed on to mobile devices and other smart devices leading to a new area of autonomous data communication devices known as Internet of Things also known as IoT . Several experts see the Internet of Things as the next industrial revolution. The Internet of Things ('IoT') has become an integral component of major metropolitan infrastructure, for example, increasing quality of life through connected healthcare, transportation, and security. The Internet of Things is also present in homes where the technology is used for home automation, such as automatic lighting, heating, and other smart devices. People use these smart devices to track their well-being and daily activities. Huge volumes of personal data are often collected and recorded as a result of the rising use of contemporary technology, and they may be used to identify the location of a person's home or office, to track habits and lifestyle, or to target advertising depending on the data subject's objectives. As technology has improved, there has been an on-going need to enact regulations that keep pace with these developments. The main aim of our research paper is to analyse the challenges that have been put forward by the IoT in the data protection sphere and how the data protection rules in the EU mainly the E-Privacy directive and the GDPR has been able to cope up with the challenges that has been put forward by the IoT. We would also look into the challenges that the data subjects would have to face in this regard and what could be the appropriate solution for these key issues.

The Internet of Things (IoT) phenomena must examine legal problems with data protection regulations. Even with the use of technologies that cannot always ensure an adequate degree of security, the Internet of Things is not immune to data protection threats. The biggest threat to privacy in the Internet of Things is profiling, which allows natural individuals to be identified using confidential information. However, there are certain concerns with possible repercussions for data security and responsibility in terms

[1] Author is a student at O P Jindal Global Law School, India.
[2] Author is a student at O P Jindal Global Law School, India.

 [ISSN 2581-9453]

of privacy and security threats. The Internet of Things system enables the flow of data, including personal data, through the Internet. The research would be divided into four main chapters. Firstly what is Internet of things and its evolution. The second chapter would deal with the EU Data Protection mainly The GDPR and E-Privacy Directive and its implications with respect to IoT. The third chapter would be focused on the Personal data Processing by IoT and Data Subjects. The final chapter would be concluding remarks and suggestion that we have put forward.

I. INTERNET OF THINGS & ITS EVOLUTION

The Internet of Things (IoT) is a global ICT (Information and Communication Technology) infrastructure that incorporates individually identifiable sensors, computing devices, algorithms, and physical artefacts known as Things. The Things will capture and transmit data through connected networks without the need for human interaction, allowing for autonomous data processing. A communication network is a critical component of an IoT (Internet of Things) infrastructure that enables information to flow between a wide range of sensors, actuators, computers, controls, and data storages. Many IoT systems need mainly one-way data transfer, while some sensor-actuator implementations need bi-directional data transfer. IoT devices could be used to assist a wide range of uses, from basic home automation tasks to life-saving activities including the use of embedded sensors inside a human body to track vital human organs. To share data among its component entities, all IoT systems rely heavily on efficient and dependable communication networks. The device profiles define the efficiency and reliability specifications of communication networks. IoT programmes allow for the storage of vast volumes of data, resulting in the creation of a Big Data archive.[3] The availability of inexpensive and minimal power computing, actuators, and communication equipment, as well as the enhancement of technological advanced software techniques that allow the execution of complex algorithms cost-effectively, have fuelled the growth of IoT systems.

Kevin Ashton of Auto-ID Labs introduced the Internet of Things idea in 1999. The original concept was to create networked networks using RFID (radio frequency identification) equipment. Since then, the term has expanded to include many new concepts, design, and implementation scenarios.[4] IoT systems are seen as distributed systems in which things or computers are distributed around different geographical areas and can share information in

[3] Janyanthi Phanindra, Internet of Things, PDFCOOKIE (Jan., 2020), https://pdfcookie.com/documents/internet-of-things-x20g1ow403l3.
[4]Jamil Y. Khan & Mehmet R. Yuce, Internet of Things (IoT): Systems and Applications (1d ed. 2019).

autonomous and efficient ways to perform a variety of activities without the need for human interaction.

Smart integration with existing networks, as well as context-aware computing utilising network services, are critical components of IoT. With the availability of Wi-Fi and 4G-LTE broadband network connectivity, the transition to ubiquitous communication technology networks is now recognisable. However, in order for the IoT objective to become a reality, computing paradigm must expand beyond conventional digital computing scenarios that utilise smartphones and portables, and into integrating ordinary existing devices and encoding information throughout the world.[5]

The Internet of Things requires common knowledge of its users and their appliances situations, technological operating systems and ubiquitous communication networks to process and communicate contextual or relevant information to where it is important, and analytics capabilities in the IoT that vision for autonomous and smart conduct. Smart integration and context-aware computing are possible with these three basic pillars in place.

Progressive evolution of today's Internet into a network of distributed objects that not only harvests information from the environment and communicates with the real world, but also incorporates established Internet protocols to offer resources for information transfer, analytics, software, and communications. IoT has emerged from its infancy and is on the brink of converting the existing static Internet into a truly interconnected Future Internet, fueled by the prevalence of devices powered by accessible wireless technologies such as Bluetooth, radio frequency identification, Wi-Fi, and telephonic data networks, as well as embedded sensor and actuator nodes.[6] From an evolutionary standpoint, the future Internet will be made up of current Internet and smart embedded objects that will serve as the foundation for the IoT. The Internet of Things would be a distinct component of the Future Internet.[7] It would be fully built into the current Internet networks, allowing the Internet's service-oriented model to make use of the system's resources. The IoT vision is that the physical and virtual worlds will become increasingly intertwined. The world is currently in the process of developing new smart embedded technologies.[8] Embedded computers are currently in the early stages of growth. This would result in an influx of real-world data,

[5] Id.
[6] Thomas Pasquier, David Eyers & Jean Bacon, Personal Data and The Internet of Things, 62 Communication of ACM 32, 33-34 (2019).
[7] In Lee & Kyoochun Lee, The Internet of Things (IoT): Applications, Investments and Challenges for Enterprises, 58 Business Horizons 431, 439-440 (2015).
[8] Shancang Li, Li Da Xu & Shanshan Zhao, The Internet of Things: A Survey, 17 Information Systems Frontiers 243, 250–252 (2015).

significantly enriching our apps and making them more aware of what is going on in the real world, in real time, everywhere.

II. EU DATA PROTECTION MECHANISMS ON IOT

The modern world has been very much focused on the aspect of privacy of the individual and protection of personal data. With the advancement in technology, the aspect of data privacy has evolved into a new sphere. The more connected a person is with technology the less is the line of distinction between the public and private sphere, and these lines are easily crossed without us noticing it.[9] With the Internet of things being a part of our everyday lives, huge amounts of user data are generated and collected for developing and improving the user experience. For this purpose, the data that are collected by the organizations are processed by them.

The European Union has a legislative structure that have been entirely built around the idea of data protection. The primary aim of these data protection regulations is to safeguard individuals against illegal acquisition, storage, and processing of their personal data.[10] The major legislation that engages with the protection of personal information in the European Union is the GDPR.[11] Any organization that processes personal data must be in compliance with it. The data that are collected by these IoT enabled devices is frequently used to enhance digital infrastructure and technologies through the gathering and the further compilation of information on users, with the purpose of using these data to provide a more convenient service to the customers.[12]

With a combination of all these data's that are collected by IoT enabled devices could be used to identify a person directly or indirectly, this would fall under the category of personal data under Article 4 of the GDPR.[13] Hence the data processing activities carried out by the IoT enabled devices would fall under the purview of GDPR.

An important mandate that the GDPR sets out is the importance of consent required to be acquired from the data subjects while dealing with personal data.[14] When it comes to the

[9] Julie E. Cohen, What is Privacy For, 126 Harvard Law Review 1904, 1905-1911 (2013).
[10] Peter Hustinx, Data protection in the European Union, 2 Privacy & Information Journal 62, (2005).
[11] Directive 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC, O.J 2016 (L 119).
[12] Jenna Lindqvist, New challenges to personal data processing agreements: Is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things?, 28 International Journal of Law and Information Technology 45, (2017).
[13] Luca Tosoni, Rethinking Privacy in the Council of Europe's Convention on Cybercrime, 34 Computer Law and Security Review 1197, (2018).
[14] GDPR. art. 4.

scenario where IoT enabled devices are in play there has been a certain ambiguity with respect to the consent framework.

Another important legislation in the European Union that would play a major role in respect to new technologies is the proposed E-Privacy Regulation.[15] This new regulation is yet to be implemented and it repeals the previous E-Privacy Directive.[16]

The major significance that the E-Privacy directive would have over the GDPR is a broader substantive area. "Article 4(3) of the proposed legislation would also include:

(a) electronic communications data' means electronic communications content and electronic communications metadata;

(b) electronic communications content' means the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound;

(c) electronic communications metadata' means data processed by means of electronic communications services for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication".[17]

While the GDPR only deals with personal data that are processed by IoT devices, the E-Privacy Regulation would also include the non-personal data i.e., machine to machine communications that are transmitted and processed by these devices that would require explicit consent from the end-users in order to transmit these communications.[18]

However, the EU has a rich legislative capacity to monitor and regulate the data protection when it comes to new technologies in theory, but the practical and real-world circumstances would be more complex.

III. REFORMS OF IOT AT EUROPEAN LEVEL

The prospects of Internet of Things to boost profitability and grow businesses has motivated merchants to engage in installing information and telecommunications systems into their commodities so that they can acquire and transfer data. Since Internet of Things is built on

[15] Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications).
[16] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002.
[17] EPRIVACY REGULATION. art. 4.
[18] EPRIVACY REGULATION. art. 8.

sensors that acquire information, there is a constant flow of data between entities. One of the most significant difficulties faced by the growth of IoT is ensuring cyber security and privacy.[19] Through the use of huge volumes of data streaming among databases, as well as confidential information sent between devices, an automated profile of the individual who is at peril of revealing this data to unauthorized parties is produced. At each level, the information collected by such networked systems is spread without the emerging consensus of the individual. As a result, personal data security is difficult to accomplish since the whole system is designed to work in a cohesive way, with the connection and interchange of information serving as a precondition for such efficiency.[20]

The Internet of Things (IoT) is a significant step toward the digitalization of the European and the European Union (EU) economy, in which devices and users are networked via communications infrastructure and exchange information regarding their state and/or the surroundings. In this regard, the European Commission has extensively collaborated with numerous organisations, along with EU Member States, during the previous six years to capitalise on the promise of IoT technology.[21] The European Commission announced the Alliance for Internet of Things Innovation (AIOTI)[22] in March 2015 to assist the development of a European Internet of Things eco-system. AIOTI was founded with the goal of contributing to the development of a dynamic European IoT ecosystem and accelerating IoT adoption. The steering Committee focus on well-defined types of industries to carry out AIOTI initiatives. Horizontal aspects include "research, innovation eco-systems, policy, standardisation, and distributed ledger technologies, as well as vertical, cross-disciplinary"[23] efforts focusing on critical IoT challenges.

The Single Digital Market Strategy was established in May 2015[24], emphasising the need to limit competition and foster accessibility for the Internet of Things in order for it to enhance economic growth. Following that, in April 2016, the European Commission adopted the "European Industry Digitization" strategy, which outlined the European union three-pillar

[19] Mauricio Paez & Kerianne Tobitsch, The Industrial Internet of Things: Risks, Liabilities, and Emerging Legal Issues, 62 N.Y. L. Sch. L. REV. 217 (2017).
[20] Larisa Antonia Capisizu, Legal Perspectives on the Internet of Things, 2018 CONF. INT'l DR. 523 (2018).
[21] European Commission, Shaping Europe's Digital Future,(Feb. 19, 2020) https://ec.europa.eu/info/sites/default/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf.
[22] AIOTI WG03 IoT Identifier Task Force, Identifiers in Internet of Things (IoT), Alliance for Internet of Things Innovation (Feb., 2018). https://aioti.eu/wp-content/uploads/2018/03/AIOTI-Identifiers_in_IoT-1_0.pdf.pdf.
[23] Digibyte, Launch of Alliance for Internet of Things Innovation, Shaping Europe's Digital Future (Mar. 9, 2021) https://digital-strategy.ec.europa.eu/en/news/launch-alliance-internet-things-innovation.
[24]Eurocities, Finding New Mechanisms For Engaging And Enabling Citizens To Make The Most Out Of Their Community, Digital Single Market Strategy For Europe (Sep., 2015) https://nws.eurocities.eu/MediaShell/media/EUROCITIES_statement_DSM.pdf .

strategy for IoT, such as the progress of an IoT ecosystem, a human-centered approach to IoT, and the establishment of an internal market for IoT. A significant obstacle to an internal market for IoT is the capacity to administer a wide variety and large number of linked devices. The twenty-first century will be defined by increased urbanisation and an increasing reliance on rapidly evolving "information and communication technologies" (ICTs). The completion of the Digital Single Market in Europe is a major aspect for attaining the goals of efficient, ecological, and inclusive economic growth. The IoT-European Platforms Initiative[25] projects are working together to define technology and development processes, as well as chances for cooperation in IoT ecosystems, in order to boost the prospects for shared strategies to application development, accessibility, and exchange of information. The shared events are designed into six task groups that were designed and implemented as part of IoT-EPI. IoT evolves over time quickly, in response to significant developments such as the ever-increasing piles of information derived and information harvesting through smart big data analysis, as well as higher prevalence of mechanisation and strategic thinking enabled by sensing devices, gadgets, and controllers especially in combination with machine learning and artificial intelligence. Furthermore to the efforts listed above, the EU has established particular objectives for Internet innovative solutions under the Horizon 2020 designed programme, the largest technology and development programme ever undertaken by the EU. The Focus Area necessitates strong collaboration among several services across multiple DGs, particularly CONNECT, GROW, RTD, AGRI, and ENER, in order to guarantee cohesive policy formulation across previously segregated economic and policy sectors.[26]

IV. DATA PROTECTION AND THE CHALLENGES IN IOT

With the tremendous advancement in the field of technology the laws that have been constituted to regulate these technologies have not been able to keep up the pace with these evolving changes.

The basic principle on which the IoT functions is its reliance on huge amounts of data. The data that are collected by these devices are known to be of personal character. Hence this character of IoT poses a new threat to the data protection mechanism and the data subjects right to determine what data is collected and how it would be used.[27] As the IoT ecosystem uses a wide range of automatic devices and sensors to identify and collect data relating to a

[25] European Platform Initiative, About IoT-EPI, (2020), https://iot-epi.eu/about.
[26] Mechthild Rohen, IoT EU Strategy, State of Play and Future Perspectives, (2018) https://www.riverpublishers.com/pdf/ebook/chapter/RP_9788770220071C1.pdf .
[27] Kai Bossen, How Technology is challenging data protection, Dmexco21 Tech & Future (Nov. 12, 2020) https://dmexco.com/stories/how-the-iot-is-challenging-data-protection/.

person i.e., location, habits, interests etc these data could be easily misused to obtain information about a data subject. The increased data gathering on the personal data would also result in illegal usage or profiling of an individual. According to the principles laid down under the OECD guidelines there are certain norms that should be followed by the data controllers while collection of data from data subjects.[28] These IoT applications can be found to be in violation of these principles which include the Collection Limitation Principle, Data Quality Principle, Use Limitation principle etc unless proper measures are taken by the stakeholders.[29]

Another area in which the IoT applications have to be strictly monitored is in the collection of data's that may fall under in the category of sensitive private information. According to GDPR the sensitive personal data are special sets of data that are to be handled with special care and specific instructions are to be followed while processing it, which include obtaining specific consent for the retrieval of these sensitive personal information.[30] With respect to IoT, there is a huge interdependence on this sensitive personal information, for example smart wearables normally do gather the data regarding health which could be prone to misuses if not properly monitored. The line of distinctions that have been given to processing of personal information and sensitive personal information would overlap under various circumstances which in turn would led to the violation of a data subject's rights guaranteed under these legislative frameworks.[31]

The Internet of Things is supposed to encourage widespread engagement of end users in mission-critical services. Smart objects are not only shift agents in terms of content and implementations. Given their ability to alter feature when they can be digitally augmented and upgraded, they can develop destructive capacity, which may have significant consequences. IoT is supposed to include a massive number of sensors that capture and transmit data about ambient conditions, physiological measurements, and system operating data. Several big problems and concerns in the areas of privacy and data safety, as well as information management are, ensuring continuity and availability in the provision of IoT-based services as well as to prevent any possible operational disruptions and interruptions.[32]

At the design point, information management, anonymity, and data protection should be

[28]OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data Privacy Principles, Digital Economy (2013) https://www.oecd.org/digital/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.html.
[29] Id.
[30] GDPR. art. 9.
[31] Lindqvist, supra note 10.
[32] Jan Henrik Ziegeldorf, Oscar Garcia Morchon & Klaus Wehrle, Privacy and the Internet of Things: Threats and Challenges, 7 Security and Communication Networks 2728, (2013).

discussed routinely, unfortunately, they are often introduced after the desired feature has been implemented this not only reduces the efficacy of the additional information protection and privacy safeguards, but it also makes them less cost-effective to enforce.[33] The greater the involvement of people in the process, the more privacy issues and practices become context-aware and situational, making them more difficult to define and determine. The detection of privacy, data protection, and security threats is dependent on the context and intent of the artefacts under consideration.[34] In general, we believe that privacy and data protection, as well as information security, are complementary standards for IoT services.[35]

V. CONCLUSION

The Internet of Things introduces a new challenge to data privacy regulation, which should be recognised in order to adopt positive reforms as a first step toward resolution. The proliferation of devices with exchanging information capabilities is bringing the concept of the Internet of Things closer to reality, in which advanced detection functions seamlessly blend into the environment and new possibilities are enabled by significant exposure to powerful descriptive information sources. The next generation of mobile networks device's progress will be decided by users' ingenuity in building new apps. In recent years, the amount of data gathered and processed by smart things has risen dramatically. The problems of using the Internet of Things have resulted in significant adjustments at the European level in terms of personal data protection. In response to these difficulties, the European Union has enacted additional laws. The Internet of Things has the potential to provide enormous advantages to customers in a wide range of domains, including healthcare, housing, transportation, and insurance. Considering the impact of technology in this growing domain, there will undoubtedly be technologies in the future that will provide unexpected advantages. Personal data must also adhere to data quality standards. As a result, they must be gathered and handled in a fair and lawful manner, which includes alerting the relevant users. Furthermore, under the purpose limitation approach, data may only be gathered for clearly described, explicit, and legal objectives that are determined prior to data processing.

IoT is an appropriate digital technology for influencing this domain by supplying new developing data as well as the computing tools needed to create innovative applications. The Internet of Things is a critical component of the future Internet because it offers the sensorial

[33] Id. at 2730.
[34] Id. at 2740.
[35] Sidi Mohamed & Sonny Zulhuda, Data Protection Challenges in The Internet of Things Era: An Assessment of Protection Offered by PDPA 2010, 4 International Journal of Law Government and Communication 01, (2019).

and actuating technologies needed to significantly improve connectivity with the physical and virtual worlds. It not only captures real-world data that fuels the entire future, but also provides actuating instruments that can make virtual-world decisions a reality. The continuing decrease in the cost of computing and networking skills suggests that the IoT will become commonplace, enabling the future Internet to reach higher levels of environmental consciousness while still making our society more knowledgeable and sustainable.

The stakeholders should accept their responsibility in the IoT infrastructure and ensure that the these technologies are made in compliance with the GDPR and other regulatory legislations. They should conduct a privacy assessment before deploying these technologies in order to calculate the risks involved and deploy such security measures that would protect the integrity and stability of the system. The major drawback of the current system is that the user's control over their data with respect to Internet of things is very limited. This could be improved by enacting a more transparent consent framework which gives the option to the data subject to specifically choose what data these devices would process. It is only by constant evaluation and evolution in the legislative and regulatory measures that IoT and these future technological advancements could be kept in check.

*****

 [ISSN 2581-9453]