Research Paper
Impact Factor: 7.184
Peer Reviewed & Indexed Journal
www.iibarr.com

IJBARR
E- ISSN -2347-856X
ISSN -2348-0653

DIGITAL ETHICS AND PRIVACY AN ANALYSIS OF THE PROBLEMS, IMPLICATIONS & APPROACHES RELATED TO DIGITAL ETHICS

Dr. Archana Ambekar* **Rekha A****
**Head,PG Department of Commerce,Jain College,Vasavi Campus,Bangalore.*
***Assistant Professor,Jain College,Bangalore.*

Abstract
The growth of information technology has greatly aided in the gathering and analysis of large amounts of data in order to draw more insightful conclusions, yet privacy remains a major ethical concern. The quick development and creation of new IT products has resulted in a lack of ethics and laws in the world of information technology. The essay aims to identify the key problems and how they affect big data analysis while also offering remedies for the current difficulties. Data collection without the owners' informed consent and careless actions by different IT corporations have seriously compromised security and best practices in the quickly expanding field. Because most IT companies have vague privacy rules, they can take advantage of the gaps in the law and circumvent established regulations. In addition, the advent of algorithms has made it simple for IT firms to establish groups that might be used for discriminatory purposes. Changes in customer behavior and technology producers can help alleviate issues affecting the IT sector and product utilization. The only alternative left is to use legislation to compel firms to comply because the companies are not taking the initiative to develop ethical practices. IT organizations' ethical compliance can be enhanced by the establishment and adoption of more complete digital ethical regulations as well as the clarification of content-related ethical systems. Data science education can be introduced to curtail the ignorance of the public by making them aware of their privacy rights.

Keywords: Information Technology, Digital Ethics, Legislation, Privacy.

1.Digital Ethics Implications On Privacy

Online social interactions and even business have been facilitated by new information technology applications, which has both advantage disadvantages. Online interactions between users and online retailers result in the sharing of a lot of data, which is gathered and analyzed by businesses for marketing purposes and organization-based decision-making without the owners' permission (Sklavos, 2017). Mass data collection through online interactions creates inferences that constitute serious privacy violations, particularly when the majority of information owners are unaware of these activities. Even more concerning is the lack of a well-defined ethical framework for digital technologies, which makes it challenging to address security and privacy issues that have been raised thus far (Sklavos, 2017). This is a result of both the quick changes in the information technology environment and the lack of supporting legislation. In order to develop solutions that guarantee a secure digital environment for all parties involved, it is necessary to address the privacy and security concerns that information technologies face. To assist stop the growing cyber insecurity, which threatens the benefits of digital technologies, such as cyberbullying and information loss, it is imperative that the relevant international bodies support international binding legislation.

Major Issues in Digital Ethics

Current big data analysis technologies violate privacy, which is one of the main issues that modern technology poses to digital ethics. These technologies are employed by corporate organizations to help

them make better decisions. (Custers, Dechesne, Sears, Tani, & van der Hof, 2018). Because the data is used to inform decisions about marketing and manufacturing, there is a substantial ethical dilemma around the use of aggregation data technology in the collecting of personal data by corporations (Damen, Köhler, & Woodard, 2017). Any personal data pertaining to biographical, behavioral, financial, medical, and biometric data obtained through business analytics is considered private. In this context, it can be summed up as follows: data analysis that is used without the permission of the information owner violates personal privacy (Bouguettaya & Eltoweissy, 2003). While there are privacy concerns regarding private data collection practices, it is not inherently improper for firms to obtain authorization from data owners. Businesses typically gather user data in order to provide more individualized services and goods to customers, thus enhancing customer care (Richards & King, 2014). . Numerous well-known companies have adopted this strategy, and some ask their customers for confirmation while collecting and using their data. Businesses, like Google and Facebook, use the model to gather data in order to tailor the user experience. However, there is an increasing number of complaints about the misuse of personal information, including sharing it with unaffiliated parties. One such instance is the most recent Facebook case, wherein the data was shared with Cambridge Analytica, an organization that utilized it for geopolitical mapping (Schneble, Elger, & Shaw, 2018). Because of the possibility of corporate misuse, such situations call into question the morality of individuals giving their informed agreement for the gathering and use of personal data.

Awareness of Data Management

In order to guarantee data accessibility, timeliness, and dependability for users, data management involves overseeing the collection, storing, validation, processing, and safeguarding of data (Bouguettaya & Eltoweissy, 2003). In today's society, technological improvements have taken precedence over awareness of the privacy concerns and issues associated with using new technologies. Because information owners are forced to consent to data collection without knowing why it is being collected, new technology applications like the Internet of Things have had a negative impact on awareness of information management and data security (Tene, 2011). Big data firms employ misleading policies to avoid obtaining consent from information owners, which results in a lack of transparency. Furthermore, regardless of the misuse of private customer data by the internet giants, it is challenging to bring any criminal charges against them due to the autonomy of the individual information user. Indeed, there is a significant ignorance of privacy policies among customers and businesses, which has allowed data-based enterprises to continue engaging in unethical actions including collecting data without the owner's consent (Clubb, Kirch, & Patwa, 2015).

Furthermore, it has proven challenging to enforce current privacy laws and owner consent requirements because to customers' passive attitude toward their rights to privacy (Steiner, Kickmeier-Rust, & Albert, 2015). It's evident that consumer behavior with regard to privacy laws and consent has been disregarded because there aren't enough restrictions in place to help the public decide whether sharing information is necessary. One reason for the low adherence to security protocols is a lack of awareness regarding the possible dangers associated with exchanging personal information with IT firms. In order to preserve privacy and enhance data management procedures, there is a need for increased awareness campaigns on the ramifications of new information technology practices and the solutions available (Riordan, Papoutsi, Reed, Marston, Bell, & Majeed, 2015).

Responsibility of IT Developers

The creation of infringing privacy information technology products and services have been blamed on developer negligence as well as the lack of awareness of the users, which makes it easy for the

developers to overlook privacy measures (Clubb, Kirch, & Patwa, 2015). There is growing government involvement in ensuring developer compliance, which has led to the rejection of products deemed as infringing on the user's privacy, irrespective of their convenience, efficiency, and positive outcomes (Cate, Cullen, & Mayer-Schonberger, 2013). Besides the irresponsibility of certain profit-oriented organizations that infringe user privacy, there is a significant gap in policies, which makes it easy for IT developers to create services and products that do not meet the established safety standards. A developer has the responsibility of ensuring that they seek consumer consent during the collection of personal information. Governments should create legislation and regulations that curb developer malpractices, by ensuring that they maintain the consumer consent requirement (Custers et al., 2018). The developers also should shoulder the responsibility of creating awareness among the information technology consumers about their need to consent before sharing information.

Group Privacy

In order to protect personal information, the emerging data analytic tools place a strong emphasis on anonymization and are primarily concerned with the behavior and lives of technology users (Taylor, Floridi, & van der Sloot, 2017). The big data era has expanded the use of data analytics, with a strong emphasis being placed on group level analysis due to the increased access that data technology techniques have allowed analysts to have, posing a privacy risk. In the current environment, there is a rise in the privacy risk associated with various social media platforms. These risks can be used in data analysis to categorize individuals into these groups, which leads to unfavorable conclusions that do not accurately reflect individual orientation and, ultimately, discrimination against those in these groups. (Taylor et al., 2017).

This highlights the need for a group-based privacy framework, which will be adequate in these situations to shield the people from discrimination on the basis of their group-based orientations. Since more algorithms are being used to classify people into categories and come to certain conclusions and predictions without actually knowing a person, more research is required to fully comprehend the privacy danger posed by social media analytics (Van den Hoven, 2017). Being part of a group, for example, can lead to negative labeling. For example, being a member of a group known to use drugs or participate in violent activities can lead to harmful profiling of individuals as being dangerous based on the grouping. The lack of sufficient data to categorize people into groups—with the majority of deductions being made based on community demographics—means that this is an intrusion on people's privacy. People disclose this information publicly on social media platforms.

2. Solutions to Privacy Issues

Regarding privacy in information technology and emerging digital technologies, there are a wide range of challenges. It is difficult to develop practical and efficient solutions due to the variety of privacy concerns pertaining to digital technology (Bouguettaya & Eltoweissy, 2003). Although there has been a lot of work in developing solutions, enacting new laws containing stricter privacy regulations is still the main strategy that can effectively limit situations of privacy infringement. Even with laws, it is challenging to completely remove unethical digital practices. Greater ability for governments to enforce the law will greatly increase compliance.

Legislation Changes

Governments all around the world can model their privacy policies after those established by the European Union (EU) nations (Custers et al., 2018). The EU develops privacy guidelines primarily by promoting openness, boosting individual engagement, enhancing developer accountability, restricting

IJBARR
E- ISSN -2347-856X
ISSN -2348-0653

and quality-managing data acquisition, and implementing safeguard-based safeguards. The European Union has ensured that enterprises comply with data collecting rules through legislation and privacy policy creation guidelines. This includes ensuring that developers and users of digital technology have the agreement of data owners (Custers et al., 2018).

b The EU makes sure that the owners of the data are informed about the information's purpose and that developers build safe databases for user data that the owners may access. These actions have played a critical role in guaranteeing the effectiveness of measure reinforcement, which can have a big impact on the development of practical ethical rules (Har Carmel, 2016). Complete transparency, device override capabilities, Internet of Things, dataset use control, and data protection are some further legislative alternatives. Thus, these solutions suggest that customers will be given greater authority to manage their personal information and that the government will become increasingly involved in information management and security.

Digital Technology Consumer Education

Increased awareness among information is necessary. Information technology users need to be made more aware of the privacy risks associated with using digital technology (Serabian, 2015). In-depth instruction can help users of digital technology combat information malpractice, which includes gathering data without the owners' permission. Public information education campaigns on information data handling practices can be launched to provide the public with awareness about data safety and reduce the risk of data loss (Kongnso, 2015). An effective education program can support the creation of campaigns for ethical literacy that can alter the current state of data privacy.by increasing awareness on the right of the information owner to give consent before their information can be used (Patwa, Kirch, and Clubb, 2015). There is a drawback in that data privacy issues cannot be completely eliminated by a brief educational program (Har Carmel, 2016). Including data privacy education in school curricula is one way to ensure sustainability. This will create a generation of data security professionals who will act as educators for those in their immediate circle, like parents and other family members who may not be aware of the risks associated with data privacy in digital technology applications (Matzner, 2018).In light of the expanding usage of digital information systems, developing a sustainable education strategy is therefore essential to maintaining data security in society.

Responsible Innovation

The EU Framework Program, which aims to promote accountability among digital technology enterprises, is credited with giving rise to the term "responsible innovation" (Gurzawska, Mäkinen, & Brey, 2017). It was created to explain the methods used in scientific research and technology development that would take into account the potential consequences on the environment and society as a whole (Gurzawska et al., 2017). Therefore, in order to properly integrate scientific and technological advancements into our society, responsible innovation is an open, interactive process that helps innovators and societal actors become mutually responsive to one another. This process is focused on the acceptability, sustainability, and societal desirability of the innovation process and its marketable products.

.

A deeper and more critical focus on accountability would be the fundamental strategy for enterprises concentrating their efforts in the IT sector; this should probably not hinder their ability to codify and execute the desired advancements in technology (Gurzawska et al., 2017). According to Van der Hoven (2017), a researcher specializing in computer ethics, responsible innovation is defined as taking into consideration the body of pertinent information regarding options and consequences as well as

evaluating them in light of moral principles like privacy, safety, and security. These are vital conditions for the creation of new technologies. The companies who are creating these policies and the customers of that specific product should both place the highest priority on implementing them. This is because the latter would have less problems with possible conflicts as mandated by the law or in the event of a privacy violation, while the former would be more secure because the maker would have given it more ethical thought.

Group Privacy

New technologies frequently bring up fresh issues for privacy protection and spark in-depth discussions on the parameters of confidentiality. The power of the individual to regulate the flow of their personal information is always at the center of these discussions. It may occasionally prove to be difficult to protect the group's privacy by using the rules that are specifically stated in legislation (Taylor et al., 2017). This is due to the fact that the numerous groupings that big data analytic generates are not particular elements seen in the real world. Therefore, comprehensive and intensive cooperative study by information analysts and ethics professionals is required to develop effective group privacy protection mechanisms.

It is necessary to modify the protocols and the approach to In order to improve privacy without having a major negative impact on performance, it is necessary to modify the protocols and technique used during considerable data processing (Taylor et al., 2017). However, there are certain steps that may be taken right now that focus mostly on enhancing individual privacy and, in turn, partially strengthening its group counterpart. Methods include the worldwide integration of data management regimes, greater data security and breach responsibility, and improved data literacy were established by Taylor, Floridi, and vander Sloot (2017). To encourage consumer involvement and control over personal data, a centralized architecture that allows users to see how their data is extended and choose how much of it is used would be ideal and admirable. [Taylor and others, 2017].

Conclusion

Regular upgrading of data privacy laws is necessary to address the evolving privacy concerns in the information technology world. Ensuring that current legislation can address both new and old information security threats should be the primary responsibility of governments. Major problems with digital information still include lack of understanding, irresponsible development, and noncompliance with established rules. As a result, addressing security issues requires a multidisciplinary approach that includes, among other things, raising developer responsibility for compliance and informing users of the need for consent, as well as other data security measures and government legislation.

References

1. Bouguettaya, A. R. A., & Eltoweissy, M. Y. (2003). Privacy on the Web: Facts, challenges, and solutions. *IEEE Security & Privacy*, *99*(6), 40-49. Retrieved from https:// pdfs. semanticscholar. org /032c/98dbf8ac0ea99943bf70175 bf8bad99950a4.pdf.
2. Capurro, R. (2009). Intercultural information ethics: foundations and applications. *Signo y Pensamiento*, *28*(55), 66-79. Retrieved from http://www.scielo.org.co /scielo.php?script=sci_ arttext&pid=S0120-48232009000200004.
3. Cate, F. H., Cullen, P., & Mayer-Schonberger, V. (2013). Data protection principles for the 21st century. [Internet Source]. Retrieved from https://www.oii.ox.ac.uk/ archive/ downloads/ publications/Data_Protection_Principles_for_ the_21st_Century.pdf.

4. Clubb, K., Kirch, L., & Patwa, N. (2015). The Ethics, Privacy, and Legal Issues around the Internet of Things. *University of California-Berkley. Last modified Spring*. Retrieved from https://www.ischool.berkeley.edu/ sites/default/files/projects/w231-internetofthingsfinalpaper.pdf.
5. Custers, B., Dechesne, F., Sears, A. M., Tani, T., & van der Hof, S. (2018). A comparison of data protection legislation and policies across the EU. *Computer Law & Security Review*, *34*(2), 234-243. Retrieved from https://www.bedicon.org/wp-content/uploads/ 2018/01/laws _topic7 _source1.pdf.
6. Damen, J., Köhler, L., & Woodard, S. (2017). The Human Right of Privacy in the Digital Age. *Publishup.uni-potsdam.de*. Retrieved from https://publishup.uni-potsdam.de/opus4-ubp /files/ 39926/srp03.pdf.
7. Floridi, L., & Taddeo, M. (2016). What is data ethics? *Oxford Internet Institute*, University of Oxford,1 St Giles, Oxford OX1 3JS, UK. Available from https://doi.org/10.1098/rsta.2016.0360.
8. Gurzawska, A., Mäkinen, M., & Brey, P. (2017). Implementation of Responsible Research and Innovation (RRI) practices in industry: Providing the right incentives. *Sustainability*, *9*(10), 1759. Retrieved from https://www.mdpi. com/2071-1050/9/10/1759/pdf.
9. Har Carmel, Y. (2016). Regulating' Big Data Education in Europe: Lessons Learned from the US. Internet Policy Review. Retrieved from DOI: 10.14763/2016.1.402.
10. Kongnso, F. J. (2015). Best practices to minimize data security breaches for increased business performance. *Walden University*. Retrieved from https://scholarworks.waldenu.edu/ cgi/ viewcontent.cgi?article=2928&context= dissertations.