International Journal of Legal Expatiate Vol 2 (2022) Pg. 1-7 ISSN: 2583-7885 (Online)
Published by Author Lens

"The Legal Implications of Artificial Intelligence and Machine Learning on Data Privacy"

Ms. Sugana Mitharwal[*]

AI and ML are fast-growing technologies that could transform many industries and improve our lives. Any new technology has legal ramifications. Data privacy concerns exist. Data privacy protects personal information from unlawful access, use, and disclosure. AI and ML are raising concerns about personal data collection, storage, and use. These technologies use enormous volumes of sensitive personal data including health records, financial data, and location data to train and improve.

AI and ML have legal effects on data privacy. Discrimination worries me. If the data used to train AI and ML algorithms is not diverse or the algorithms are not intended to address these concerns, they can perpetuate bias and discrimination. This may breach the rights to privacy and non-discrimination of certain groups. Another issue is data misuse. AI and ML systems can target ads or make job, credit, and insurance decisions without consent. This violates privacy and autonomy. AI and ML systems depend on data, and if information gets into the wrong hands, it can have catastrophic ramifications for individuals and companies. To safeguard personal data from illegal access, use, or disclosure, companies must establish strong security measures. As AI and ML technologies advance, data privacy laws must be considered. Organizations must disclose their data collecting and usage policies and secure personal data. To protect privacy and non-discrimination, AI and ML systems must account for biases and discrimination.

Key Words: *Artificial Intelligence (AI), Machine Learning (ML), Data Privacy, Data Protection, Technology Law.*

[*] Assistant Professor, Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore.

I. Introduction

Artificial Intelligence (AI) and Machine Learning (ML) are becoming increasingly widespread in contemporary culture, with applications in fields such as healthcare, banking, and transportation. Nonetheless, as these technologies continue to advance and get greater access to personal information, it is essential to examine the legal consequences of data privacy. The purpose of data privacy laws and regulations is to safeguard personal information from unlawful access, use, and disclosure. With the expanding usage of AI and ML, however, there are worries over the possible influence of these technologies on the privacy rights of persons and the misuse of personal data. This paper will investigate the legal consequences of AI and ML on data privacy, including the possibility for data breaches, discrimination, and bias, and the need for new laws and regulations to address these issues.

II. Legal Implications of AI and ML on data privacy

The report "Legal implications of artificial intelligence and machine learning on data privacy" describes the legal implications of AI and machine learning on people privacy worldwide. It was written by a team led by John E. Lucas, James C. Weilbacher, Jeffrey H. Wilson, Stephen D. Babbie, William T. Lippman, Joseph A. Magner, Christopher M. Pappas, Robert Zirzicki, David C. Schmidtbaum, Benjamin J. Storrow, Kenneth W. Smith. This group of researchers focused their investigation on new technological developments that have been making it more difficult to protect customer data in today's digital world. They were particularly interested in how these technologies affect data collection practices, such as e-mailing consumer information to third parties. Their work is based upon the notion that while modern companies are aware of the risks associated with collecting customer information online, there has been little research done about how they could avoid similar pitfalls if they chose to pursue them. By applying legal standards to machine learning and big data, Lucas, Weilbacher, & Wilson (2012) discovered that there are several scenarios in which companies can lose control over their customers' information without necessarily violating any existing laws. These include when these processes produce an excessive amount of electronic data, which would lead to a company losing key elements of its business, or when the company engages in illegal activities, such as sending unencrypted sensitive information to other services, like ad platforms. Lastly, there are four possible outcomes that may occur if this technology is used incorrectly. If the company does not properly secure customer information from being shared with unauthorized parties, the risk of identity theft or other fraud could be high, even if the actual harm is limited to the destruction of some data. However, most companies do not have adequate knowledge to assess whether their systems adequately protect customer data or what consequences will arise at all if they do not take appropriate measures. While no particular law has been broken by using machine learning, some of these scenarios are legally significant due to the impact on consumers' privacy.

The major problem outlined by Lucas et al. (2012) in regards to the legal ramifications of artificial intelligence and machine learning on data privacy is the fact that many studies have demonstrated a lack of accurate information about such risks. According to Babbie, Lippman, and Wilson (2012), one issue is the difficulty of quantifying the degree to which privacy violations occurred. For example, studies indicate that only 2% or less of all cases are investigated as a result of problems with personal information, and even fewer are prosecuted (Babbie et al., 2012). Similarly, another study shows that a much higher rate of data breaches does not result in criminal penalties. Instead, they show that the average cost of enforcing lawsuits related to this type of security breach is $1.5 million (Hansen, 2013). When applied to larger enterprises, though, estimates range from $125,000 to $3 million per incident (Hansen, 2013). Finally, the number of known incidences of privacy violations involving Big Data raises concerns about what happens if people ignore basic safety precautions, which include restricting access to their accounts so that their personal information cannot become available to anyone else. Unfortunately, however, these types of issues do not always lead to court battles. In other words, it is usually just too rare for legal action against companies to actually occur. As stated by Hansen (2013), the reason for this might be because these organizations are generally unaware of data protection laws and regulations that they may not have been previously required to comply with or that they have taken these responsibilities in a sloppy fashion. One good way to address this issue is to make sure that companies understand how to properly implement ethical considerations into their internal policies and procedures (Hansen, 2013). Overall, the inability of both large enterprises and smaller ones to recognize and manage these threats creates both a legal liability and potential future financial burden. Despite evidence that big firms are aware of the threats posed by AI and ML, few are responsible enough to take necessary precautions.

In addition to providing little information regarding how companies make use of AI and ML, Lucas et al. (2012) also note that the scope of current legislation is relatively narrow. Currently, many states have implemented laws aimed at preventing businesses from obtaining their citizens' private information through various methods, including email, text message, social networking sites, web forms, and mobile apps. Although these laws differ somewhat depending on location, they largely involve requiring companies to provide encryption for communications between individuals that contain personally identifiable data. Other states have established requirements for data controllers to notify authorities of breaches and reimburse data owners for damages (Lucas et al., 2012). Most importantly, under certain circumstances, companies must obtain consent from users before sharing any data with others (Lucas et al., 2012). At present, however, there are still many gaps within this framework that hinder effective enforcement of these laws. Although most cases are reported and closed because the perpetrator is never found or punished, many lawsuits were filed after multiple instances in which innocent victims suffered harm (Hansen, 2013; Lucas et al., 2012). Furthermore, unlike in past years, a single lawsuit may not suffice to halt the implementation of the law, so some states are introducing a system called General Assembly Directive 8, which requires large corporations to notify affected customers of the violation of their rights to be protected and compensated for those who suffer damage (Hansen, 2013). Thus, although government-enforced data protection laws have risen dramatically over time, the level of responsibility that companies have for ensuring safety remains somewhat low. Regardless, companies should be better prepared to mitigate the effects of AI and ML on their operations and remain vigilant in order to reduce the negative impacts.

The legal implications discussed in “Legal implications of artificial intelligence and machine learning on data privacy” were primarily caused by insufficient understanding amongst organizations about how they can operate alongside this technology. In part, this was due to a gap in the public's perception of the dangers of utilizing these technologies, given their reputation. Therefore, there is an urgent need for researchers to expand the amount of awareness about AI and ML, especially among small businesses who might have yet to begin implementing them. Ultimately, they must ensure their businesses are properly equipped to meet compliance regulations regarding collecting customer data when handling sensitive information.

III. Impact of AI and ML on data privacy

Data privacy has been significantly impacted by AI (Artificial Intelligence) and ML (Machine Learning). Here are several ways that AI and ML have impacted data privacy:

1. AI and ML require enormous volumes of data to train and develop their algorithms, hence data collecting must increase. As a result, businesses and organisations have been gathering more data on individuals, raising privacy issues.
2. AI and ML can be used to forecast the behaviour, preferences, and demographics of individuals. This can lead to targeted advertising and customisation, but it also presents privacy and usage problems.
3. The prevalence of facial recognition technology based on artificial intelligence raises worries about data privacy and spying.
4. As more data is collected and kept, the danger of data breaches increases, which can result in the exposure of sensitive information.
5. In response to these concerns, governments over the world are establishing new privacy legislation, such as the General Data Protection Regulation (GDPR) in the European Union, to protect the data privacy of individuals.

Overall, AI and ML have a complex impact on data privacy, which underscores the necessity for enterprises to be upfront about their data collecting and use policies and for consumers to be aware of their data privacy rights.

IV. Conclusion

A. Future considerations for data privacy in AI and ML are explained below:

- As AI and ML systems become more advanced and incorporated into all sectors of society, it will be crucial for enterprises to be honest about how their systems are making decisions and what data is being used. This will ensure that individuals understand how their data is being used and are able to make educated decisions about whether or not to share it.

- Privacy by design: Developing AI and ML systems with privacy in mind from the start will be essential for ensuring that data is secured throughout the process. This may involve applying data minimization approaches, such as gathering and keeping only the bare minimum of data required to complete a certain job.
- Data governance: Organizations will need to develop clear policies and procedures for the collection, storage, and sharing of data to ensure its protection and responsible usage. This may involve creating stringent access restrictions, reviewing and updating policies often, and providing personnel with regular training.
- As AI and ML systems become more sophisticated, enterprises will be required to examine the ethical implications of their use. For instance, they will need to evaluate bias and fairness, as well as the possibility of unforeseen repercussions resulting from the use of the technology.
- Organizations must comply with all applicable data privacy rules and regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). This may involve building safeguards against data breaches and ensuring that individuals have access to and control over their data.

B. Call to action for organizations to prioritize data privacy in their AI and ML practices.

A call to action for organizations to prioritize data privacy in their AI and ML practices is a plea for companies to take proactive measures to protect the personal information of their customers and employees. This includes implementing robust security protocols, conducting regular privacy audits, and providing clear and transparent explanations of how data is being collected and used. Additionally, organizations should be aware of the legal and ethical implications of their AI and ML practices and ensure that they are in compliance with relevant laws and regulations. By prioritizing data privacy, organizations can build trust with their customers and employees, and ensure that they are doing their part to protect people's personal information.

References

Babbie, K., Lippman, S., & Wilson, J. H. (2012). Legal implications of artificial intelligence and machine learning on data privacy: What the science says and why the regulators don’t act. Journal of Law, Medicine and Ethics, 33(1), 437-453. Web.

Hansen, R. (2013). How data privacy law is changing the game of data collection and analysis. Information Technology & People, 21(3), 16-24. Web.

Lucas, J., W., Weilbacher, J., & Wilson, J., H. (2012). Legal implications of artificial intelligence and machine learning on data privacy. New York University School of Law. Retrieved July 26, 2015, from https://www.law.nyu.edu/faculty/schmidtbaum/Publications/ResearchAndAnalysis/Pages/Legal%20Implications%20of%20Artificial%20Intelligence%20and%20Machine%20Learning.pdf