WHITE PAPER FOR REGULATION  
CS 370 Current/Emerging Trends in Computer Science

Sergio Mateos

Sothern New Hampshire University

As technology develops at a fast rate, the problem of many situations occurs with it, from bugs to regulations. For this reason, is crucial to follow and execute every regulation to protect the integrity of the users and provide transparency in the company. As part of one of the engineering teams in a major social media network, we take regulations and restrictions solemnly. As part of the transparency of the company, I will break down the problems to clarify any problem with the General Data Protection Regulation (GDPR)

Neural network is a collection of algorithms learning systems that use a network of functions to collect, understand, and translate data input from one to another one. The concept of neural network is inspired by the neurons from the human brain which translate information for the body to function. According to IBM "Deep neural networks consist of multiple layers of interconnected nodes, each building upon the previous layer to refine and optimize the prediction of categorization." (Yahoo New, 2023). The structure of the neural network is conformed of three layers: input, hidden, and output.

* Input layer: The input layer collects the data and translates it to hidden layers.
* Hidden layer: The hidden layers process the data and compute it in nodes. The node creates actions that create specific purposes.
* Output layer: The output layer takes the processed data and creates results.

“Neural networks are being applied to many real-life problems today, including speech and image recognition, spam email filtering, finance, and medical diagnosis, to name a few.” (DeepAI, 2017)

The use of neural networks is common in many aspects of our life, for example, business uses customer data to maximize the experience and satisfaction of the users by providing recommendations based on their necessities or interests. Neural networks are used to create models based on customer interest and calculate different possibilities as a result. The precision of these models can help the users have better options based on their criteria. Amazon is a tech leader in these types of neural network models. Amazon provides different types of items based on your search history or criteria and suggests items that you might need to complement the first item. For example, if I want to buy plates, the neural network model will suggest spoons, knives, or even cups. “Company leaders saw a need to use data and machine learning to deliver on customer promises and achieve cost-effective functionality at scale. With those goals in mind, Amazon.com set out to become an AI-driven leader in product forecasting.” (Forbes, 2021).

As we analyze the pros, we also need to understand their cons, several ethical issues can be hidden especially if the algorithm is unknown to the users. Potential concern arises from “black box”, Artificial Intelligence (AI) systems with internal working that are invisible to the users when the algorithms are designed for patterns and not for bias. Black box allows the user to see the input and the output, but the process would be invisible to the user, which the process may not consider biased or misunderstand the information and produce a wrong result. The report made by Harvard Business Review called “AI Can Be Both Accurate and Transparent” reports how big companies are using AI to generate decisions that often result in inaccurate or completely wrong. This approach creates real risk. “Research has shown that a lack of explainability is both one of executives’ most common concerns related to AI and has a substantial impact on users’ trust in and willingness to use AI products — not to mention their safety.” (Candelon, 2023).

Many organizations, laws, and regulations are created to protect users from the abuse of big corporations like GDRP. The General Data Protection Regulation (GDRP) is one of the strictest sets of rules on data protection and privacy that are based on the European Union. GDRP has seven principles which are: transparency, purpose limitation, data minimization, accuracy, storage limitations, confidentiality, and accountability.

* Transparency: Organizations and companies are required to provide clear and consistent information to their users about the management of their data, and how is being collected, processed, and stored. Also, users need to be informed if the data is being used and reused and the process.
* Purpose Limitations: The data would be collected and processed for specific and legitimate purposes. Companies and organizations have a limitation of how much data will be collected to not exceed more than necessary.
* Data minimization: The data will be limited to ensure that companies are not collecting more than necessary. The data collected will be adequate and relevant for the only purpose that is being collected.
* Accuracy: The data will need to be updated constantly. Also, the data will always need to be correct.
* Storage Limitations: The data collected would be stored for no longer than the necessary time.
* Confidentiality: The data would be managed in a manner that will contain the proper security, including protection against unauthorized/malicious users, leak, damage, or destruction of information. The confidentiality of the information will need to be ensured by the companies and organizations.
* Accountability: Companies and organizations will demonstrate compliance with the GDRP rules. Companies and organizations will need to implement all the necessary tasks like conducting data protection or appropriate techniques to ensure that the users’ data would be always protected.

As the lead engineer for a major social network company, understanding the importance of GDPR law is crucial for the integrity of our customers and the success of the company. Analyzing the GDPR I can highlight specific legal concerns that we are going to be more careful to follow since we interact directly with them.

* Accountability: As a company, managing a large amount of data could be difficult if it is not handled properly. The leaking of data could easily happen on both sides from the company security default or by accident. In any scenario, we need, to be ready to be honest with our customers and responsible for this accident.
* Storing limitation: The use of a neural network will require a large amount of collection of data to output a result as accurately as possible. The limitation of time on the data storing could affect the neural network since we might dispense some information that could be beneficial in the future.

As part of the regulation, the company will ensure the minimization of bias for accurate results, preserve all the personal information for the company, communicate to the user for feedback, and create a better experience.

Data collection is a crucial part of our business model, since our goal is to provide the most accurate information, suggestions, and analysis to our customers, collecting data is a crucial part of our business model. Customers may think that the collection of their data is a violation of their privacy, and they will be manipulated to buy or look at certain articles. All these arguments are valid and understandable since they trust us and use our service thinking that they will be safe, in which case they are since our main goal is to provide accurate information to our customers and satisfy their needs.

Our company focuses on the satisfaction of our customers and the benefit from our platform, to be a social media platform is very challenging since every improvement that may go to be implemented, first, need to be analyzed to make sure it’s safe for our customers. Our team is fully dedicated to following and obeying the GDPR law. Currently, GDPR tracks the new trends in Artificial Intelligence (AI) and Machine Learning (ML) aiming at private information and ethics. Our team will focus first on transparency with our customers about their information, notify them that the data would be used for a specific reason, and after that, the data dispense in a safe way. The data would be encrypted, and a security team would be focused on the preservation of customer information.

Reference

*With artificial intelligence growing popular, here’s what to know about how it works*. (2023, May 21). Yahoo News. <https://news.yahoo.com/artificial-intelligence-growing-popular-heres-090139612.html?fr=sycsrp_catchall>

*Build with AI* | DeepAI. (2017). DeepAI. <https://deepai.org/machine-learning-glossary-and-terms/neural-network>

Contributor, A. W. S. (n.d.). *Amazon Web Services BrandVoice: Predicting The Future Of Demand: How Amazon Is Reinventing Forecasting With Machine Learning*. Forbes. Retrieved May 23, 2023, from <https://www.forbes.com/sites/amazonwebservices/2021/12/03/predicting-the-future-of-demand-how-amazon-is-reinventing-forecasting-with-machine-learning/?sh=4e31cc501b6b>

Candelon, F., Evgeniou, T., & Martens, D. (2023, May 12). *AI Can Be Both Accurate and Transparent*. Harvard Business Review. https://hbr.org/2023/05/ai-can-be-both-accurate-and-transparent