Kennedy Uzoho

Southern New Hampshire University

CS 370 AI/ML

Project One Submission

Neural networks are a type of machine learning algorithm that is modeled after the structure and function of the human brain. They consist of layers of interconnected "neurons," which process and transmit information.

The input layer receives data, such as an image, and passes it through the hidden layers where the neurons process the information and learn from it. The output layer then classifies the object by identifying a picture as a dog or cat.

Neural networks are often used to create personalization in the user experience, such as recommending products or content based on a user's browsing history. However, this can raise ethical concerns such as hidden biases in the system. For example, if the dataset used to train the algorithm is skewed towards a certain demographic, the system may perpetuate discrimination.

The General Data Protection Regulation (GDPR) has provisions that affect personalization. For example, transparency requires that individuals be informed about how their data is collected and used. Purpose limitation requires that data can only be used for specific, explicitly stated purposes. Data minimization requires that data be collected and stored only to the extent necessary for the purpose it is being used for. Accuracy requires that data be kept accurate and up to date. Storage limitation requires that data be deleted when it is no longer necessary for its purpose. Confidentiality requires that data be kept secure. Accountability requires that the controller be able to demonstrate compliance with the GDPR.

A company's use of neural networks to personalize the user experience may raise legal concerns under the GDPR. For example, if the company is not transparent about how it collects and uses data, it may be in violation of the transparency principle. Not collecting data may not be a possibility for the company's business model, but it is possible to minimize the amount of data collected and to ensure that it is only used for specific, stated purposes.

One trend in artificial intelligence and machine learning aimed at preserving privacy is differential privacy. This technique adds random noise to the data to mask individual information while still allowing for useful insights to be gained from the dataset as a whole. Another trend is federated learning, where the model is trained on the user's device rather than on a central server.

To comply with GDPR, a company could propose changes such as implementing differential privacy techniques in their data collection and storage process. They could also ensure that data is only used for specific, explicitly stated purposes, and that individuals are informed about and have control over their data. Additionally, the company could implement a process for regularly reviewing and updating its dataset to ensure accuracy. In compliance with the GDPR, the company must appoint a Data Protection Officer (DPO) to oversee and monitor the company's compliance with the GDPR and to advise on privacy-related issues.

References

Narayanan, R. (2021, December 28). *Understanding key terms in AI*. Medium. Retrieved January 8, 2023, from https://medium.datadriveninvestor.com/understanding-key-terms-in-ai415baa8b37a1