Neural Networks Explained

Machine learning is a branch of artificial intelligence that utilizes data and algorithms to imitate how a human might learn a particular idea or concept. Neural networking is actually a sub-field of machine learning that uses a network of nodes and a process data a particular way in order to achieve a desired end result. The term “node” or “neuron” is borrowed from that fact that these networks behave in a similar, yet significantly simpler and mathematical way that a human brain neuron might when processing information. Each node contains weights, variables, threshold, and an output that all function as an overall formula to process data. A simple neural network can be broken down generally into three distinct, interconnected layers: an input layer, hidden layer or layers, and an output layer.

An input layer is where data is fed into the network so that the process of performing operations on the data can begin. Simply put, the data is processed based on the various factors mentioned previously, and if particular conditions are met during this process, the output is passed onto the next layer of nodes in the network.

The hidden layer or layers come after the input layer and before the output layer of nodes in the network. This layer is generally what handles the majority of the computations and passes output data along each of its layers if certain conditions are met based on configuration. Each node that is performing computations is attempting to understand the data in a particular way in order to produce the desired final output. If we have a significant amount of hidden layers, sometimes this is referred to as a “deep” network.

The final layer, known as the output layer, is the final output of the network’s computations, which is the result of the input data being manipulated to make a particular prediction.

Neural Networks and Personalization

Using the process described previously, neural networks can be fed a particular set of data and output a predictions based on this data. Oftentimes for a simple neural network explanation, the example of an image processing system or number prediction system is used to illustrate how an AI model can be trained to identify images or numbers based on an initial input. However, the behavior of how a user navigates pages, what they click on, or how long they spend on a particular element on a website can all be broken down statistically and insert into a neural network to be processed.

Based on a user's behavior, a neural network can deliver various outputs than can personalize a user's experience when utilizing a service. If, for instance, a user has watched particular videos that are cataloged in a specific way within the service's database, an AI algorithm can be used to predict, based on this behavior, what a user might want to watch next. These outputs can then be used to recommend videos to the user that will likely have a higher probability of being viewed due to their personalized nature.

One of the most significant ethical concerns that this type of system may bring along with it is the breach of privacy that occurs. In order for the neural network to properly recommend personalized content to the user, their usage habits must first be identified and collected. Often times, users generally do not know or understand how their data is being used or store, or it may be ambiguous that their data is even being collected. Users may not be appropriately informed that all of their habits are being tracked and processed in an AI system to be used in various ways. This presents the ethical dilemma of wrongfully collecting a user's data and manipulating the user with personalized content without their direct, informed approval.

GDPR Statutes and the Effects on Personalization

GDPR or General Data Protection Regulation is a European Union law that serves to regulate the ways data is collected, processed, and stored on citizens of its domain. In regards to data collection for personalization, GDPR requires that websites or organizations must first request the consent of a user before collecting their data, outlining how it may be used by their service. Here are four relevant articles, briefly described from the GDPR guidelines, that might have an impact on the personalization of user experiences:

- Article 5 Principles relating to the processing of personal data: Among the various principles outlined, the first states that personal data must be processed lawfully, fairly, and in a transparent manner. This would indicate that in order for the company to collected data for personalization, they must first ensure it is collected according to that law and that the user is informed how, what, and why this data is to be collected. The "how" component can also involve how the data is processed in the algorithms, meaning there would be a need to explain how the personalization is brought about with their data (black box).
- Article 21 Right to object: This article states that a user always has the right to object to their data being collected or processed at any time. In regards to collection for personalization, this means that a user has the right to refuse their data being collected and thus removing the ability for the service to be personalized based on user behaviors.
- Article 7 Conditions for consent: The entity that is collecting user data must have the ability to provide proof that the user has consented to their data being collected. If a user gives consent for their data to be used to personalize the service they are using, the company must prove that this consent was given.

- Article 17 Right to erasure: If a user requests it so, any data that was collected after a user previously consented to the collection must be deleted and removed based on specific guidelines. This means that if user behavior was tracked and processed for personalization after consent, upon the request of the user, this data must be deleted.

As mentioned previously, neural networks rely heavily on processing this user data in order to customize the experience of a website or service. Based on some of these statutes that GDPR outlines, it would be imperative for the company to follow these guidelines if they do not wish to receive legal repercussions from the European Union for misusing data of their users. Explicit consent and transparency must first be established with the user before the process of tailoring the service through the use of neural networks can begin. This posits the question: Is the business model of targeted advertising possible without collecting user data?

There are some ways that targeted advertising can be achieved without the use of collecting personal data. One significant way would be what is known as demographic advertising. Rather than collecting data on the behavior of user whilst they browse a particular webpage or service, the context of the service itself can be used to choose an appropriate advertisement collection. For instance, if the service being offered by the company is some sort of web-based game, that service will generally offer a certain demographic of gamers. It would then be reasonable to assume advertisements targeted towards gamers using the service would be appropriate, with no data on each individual player needing to be collected.

Adaptations and Final Thoughts

To be perfectly clear, the business model the company has of collecting user data in order to provide personalized experiences and targeted advertisements is absolutely viable under GDPR law. The guidelines under GDPR outline the process that must be followed in order to

protect user data and give the user more control of how their data is implemented by third-parties. If these clear guidelines are followed, it is possible for the company to continue the same operating procedure within the European Union, lest they receive significant financial or operating penalties from the governing body.

These procedures may involves explicitly informing the user what data is to be collected and how it is to be used, only collecting data when explicit consent is given, honoring the user's rights regarding the requests of their data within guidelines, and following the proper procedures regarding storing, handling, and security of user data. Other procedures that are more centered around the techniques used when processing data in machine learning involve utilizing less data to reach a similar end goal in the form of matrix capsules, encrypting data that is sent through AI systems, and providing systems that explain how outcomes are achieved. However, in order for this approach to work, each of these guidelines and policies must be followed without exception. This means that if at any time a user revokes consent for their habits to be tracked and requests their data be deleted, the business model of using data to create personalized experiences cannot be implemented if GDPR is to be respected. In this event, the company must seek ways of targeting users for advertisement through other means that do not involve data collection, such as the potential for demographic advertising if the services offered by the company are known to be used by specific users from a particular demographic.

References

Andrew D Selbst, Julia Powles, Meaningful information and the right to explanation, *International Data Privacy Law*, Volume 7, Issue 4, November 2017, Pages 233–242, https://doi.org/10.1093/idpl/ipx022

Demographic targeting. Know Online Advertising. (n.d.). https://www.knowonlineadvertising.com/targeting/demographic-targeting/

IBM. (n.d.). *AI vs. Machine Learning vs. Deep Learning vs. neural networks: What's the difference?* IBM. Retrieved from https://www.ibm.com/cloud/blog/ai-vs-machine-learning-vs-deep-learning-vs-neural-networks

IBM. (n.d.). *What are neural networks?*. IBM. https://www.ibm.com/topics/neural-networks

Intersoft consulting services AG. (n.d.). *General Data Protection Regulation* . gdpr-info.eu. https://gdpr-info.eu/

Newman, T. (2017, December 7). *Neurons: What are they and how do they work?*. Medical News Today. https://www.medicalnewstoday.com/articles/320289

Southern, M. G. (2023, May 16). *OpenAI CEO on AI Oversight: From Disinformation to data privacy*. Search Engine Journal. https://www.searchenginejournal.com/sam-altman-on-ai-oversight-balancing-risks-advancements/487098/#close

Ved, A. (2019, February 28). *How to develop artificial intelligence that is GDPR-friendly*. TechGDPR. https://techgdpr.com/blog/develop-artificial-intelligence-ai-gdpr-friendly/