Neural networks are computational models inspired by the human brain's structure and functioning. Like the billions of neurons and synapses in our brains, neural networks consist of algorithms that interpret relationships within data. Comprising input, hidden, and output layers, these networks classify objects based on data input. The input layer stores initial data, which is then processed and computed in nodes within the hidden layer. Finally, the output layer classifies the object and produces a corresponding output. They interpret data relationships to enhance user experiences through personalization. However, concerns of an ethical nature arise in relation to the collection of data and the potential for biases. To address these concerns, the General Data Protection Regulation (GDPR) safeguards personal data and emphasizes principles such as transparency, purpose limitation, and accountability.

Neural networks play a crucial role in personalization, enhancing the user experience. Each user has unique preferences, and platforms strive to cater to those preferences. For instance, platforms like TikTok employ neural networks to analyze user data, including liked videos, followed accounts, searches, and history. This data is processed to generate a stream of personalized content and targeted advertisements, tailored to individual interests. However, while personalization offers benefits, ethical concerns arise regarding data collection, storage, and the potential for biased outcomes.

To address these concerns, the General Data Protection Regulation (GDPR) establishes laws and regulations to safeguard personal data and empower internet users. The GDPR defines personal data as information specific to an individual's private, professional, or public life. Companies are required to obtain user consent before collecting and processing personal data. The regulation emphasizes principles such as transparency, purpose limitation, data minimization, accuracy, storage limitation, confidentiality, and accountability.

Transparency ensures that companies are open and honest about why personal data is being processed. Purpose limitation specifies that data should only be collected for explicit and legitimate purposes. Storage limitation sets guidelines on how long companies can retain personal data, requiring justifications for retention periods. Confidentiality ensures the secure handling of personal data, while accountability mandates companies to maintain records and measures to comply with data processing principles.

The GDPR poses challenges for companies that rely on neural networks to personalize user experiences. For example, strict storage limitations may impact the duration of data retention. Failure to comply with GDPR principles can result in legal consequences, such as fines and damage to a company's reputation. Not collecting data altogether is difficult for companies with business models dependent on user data. Nonetheless, GDPR compliance fosters privacy, establishes best practices in AI and machine learning, and builds a trusting relationship between users and personalized AI systems.

Overall, neural networks provide powerful tools for personalization, artificial intelligence and machine learning, but their use raises ethical concerns. This includes allowing people to request their data and say no to companies to sharing their data. Giving users the chance to take their data away whenever they want. Neural networks have revolutionized the fields of artificial intelligence and machine learning by learning from labeled data. Deep learning enables the creation of intricate representations, while convolutional neural networks excel in tasks related to computer vision. Ethical considerations include addressing biases, ensuring fairness, enabling interpretability, and providing explanations for model decisions. Continual learning is focused on the adaptation of neural networks to new data. Compliance with the GDPR ensures responsible practices and fosters trust between users and AI systems. The GDPR serves as a crucial framework to protect personal data and ensure responsible practices in the era of AI-driven personalization.

References

*Artificial Intelligence (AI): Introduction, Future 2023 - Prakash Thakur*. (2023, July 12). https://imprakash.com/artificial-intelligence/

‌ Bccat337421. (2023, June 1). *GDPR - Safeguarding Data Privacy & Building Trust*. BitConcat. https://bitconcat.com/gdpr-safeguarding-data-privacy-building-trust/

‌ Wolford, B. (2018). *What Is GDPR, the EU’s New Data Protection law?* GDPR.eu; European Union. https://gdpr.eu/what-is-gdpr/

‌ *The three challenges of AI regulation*. (n.d.). Brookings. https://www.brookings.edu/articles/the-three-challenges-of-ai-regulation/

‌ Candelon, F., Carlo, R. C. di, Bondt, M. D., & Evgeniou, T. (2021, September 1). *AI Regulation Is Coming*. Harvard Business Review. https://hbr.org/2021/09/ai-regulation-is-coming

‌