BRITISH ACADEMY OF MANAGEMENT Continental Network

Artificial Intelligence in our Private Lives – A Trade-Off between Simplicity and Security?

Christian-Andreas Schumann[1], Vanessa Reiher[1], Anna-Maria Nitsche[1,2], Kevin Reuther[1,2]

[1] *University of Applied Sciences Zwickau, Kornmarkt 1, 08056 Zwickau, Germany*

[2] *University of Leipzig, Augustusplatz 10, 04109 Leipzig, Germany*

AI has become an essential part of people's everyday lives, as it proves to be convenient in many aspects. Smart home devices understand our language and act based on the given com-mands. Face recognition allows users to unlock their phone without lifting a finger. Chatbots facilitate contacting customer services by making it possible to avoid queued calls. There are many more examples to be presented here, but the underlying idea is apparent: AI has a facilitating effect on many aspects of life and is slowly becoming too comfortable for many people to imagine their life without it. In this context the reliance of AI on the use of data and what that means for consumer privacy comes into question. Is the risk of data theft and misconduct or invasion of privacy greater than the facilitating effect of AI? Is collecting large amounts of data from people ethically acceptable? This blog post attempts to provide some potential answers to these questions.

As is known by now, AI systems rely on the use of data, which comes with great responsibilities for AI developers. Customers need to be informed on how and why data are being accessed. The consumer should have the right to deny data access, even if that entails a decline in the performance of an AI system. This idea relates to the concept of data sovereignty, which expresses the data owner's right to autonomy and self-determination concerning the use of private data (Knittl, Neuberger and Dieterle, 2020). Furthermore, it is the responsibility of the AI developers to treat collected data responsibly. This can be stipulated in special regulations, such as the General Data Protection Regulation of Europe, which specifies rules and limitations when handling sensitive consumer data. All of the factors mentioned above could constitute an ethical way to access and handle consumer data.

However, even with laws for data protection in place, there is an "obvious trade-off between delivering information to data users and protecting the privacy of individuals" (Schmid, 2010, p. 64). The trade-off occurs between the facilitating effect of AI and the consumers' privacy. Depending on the kind of data collected, this trade-off might be more or less severe. While some data obtained by AI systems may be of little significance or not regarded as private, other data can indeed be sensitive and personal, such as information on health. During the data gathering process, differentiation between these two data types can often not be achieved and the systems tend to obtain non-sensitive and sensitive data simultaneously (Cataleta, 2020). It is thus the responsibility of the AI producers to treat the obtained data in a way that is ethically acceptable and lawful, as previously mentioned.

Due to the existence of laws and regulations and because AI is used to create advantages for consumers, the need to access private data can be viewed as ethically justifiable. AI offers a multitude of possible applications and is therefore generally advantageous. However, if the wrong people gain access to this technology, it can be used for deception and fraud (Jin, 2019). Since data monitoring and collecting is enabled by constant connectivity to the Internet, fraudulent access from third parties is possible (Cataleta, 2020). Hence, the security of the data needs to be guaranteed. The lack of consumer privacy in connection with data leaks pos-es an opportunity for companies to produce solutions as safety precautions (Elvy, 2017). Such systems could be advantageous to the further development of AI as they may fix one of its major flaws. However, the degree to which such solutions might offer security remains questionable.

As of today, society may not yet be at a point where consumers need to implement AI into their everyday lives at all times. Thus, they are still left with a choice when it comes to the trade-off between privacy and convenience. Even though AI has been established in many areas already, its development is far from being completed. There are various open questions concerning the implementation and development of AI, one of them being the privacy aspect. In the future, this topic will demand much attention and extensive research.

References:

Cataleta, M. S. (2020) 'Humane Artificial Intelligence - The Fragility of Human Rights Facing AI'.

Elvy, S.-A. (2017) 'Paying for privacy and the personal data economy', Colum. L. Rev., 117, pp. 1369.

Jin, G. Z. (2019) 18. Artificial Intelligence and Consumer Privacy. University of Chicago Press.

Knittl, S., Neuberger, V. and Dieterle, S. (2020) 'Das Internet of Things-zwischen Usability und Verlust der Datensouveränität', HMD Prax. Wirtsch., 57(3), pp. 558-570.

Schmid, M. (2010) 'Data Mining in Large Databases—Strategies for Managing the Trade-Off Between Societal Benefit and Individual Privacy', Advances In Artificial Intelligence For Privacy Protection And Security: World Scientific, pp. 63-80.