Conflicts between artificial intelligence and data protection regulation

Authorship: Manuel David Martín Rodríguez
20th September 2019

Introduction

I will begin this publication with a cite of the recently deceased and former European Data Protection Supervisor Giovanni Buttarelli: “GDPR is not an obstacle for Artificial Intelligence or any technology designed to serve humankind, but training Artificial Intelligence requires enormous quantities of personal data. Accountability cannot be delegated to a machine, you have to take responsibility for consequences, foreseen and unforeseen”.

If we analyse this statement we will discover that it is mandatory to be careful about the use of data by artificial intelligence systems. With the new data protection regulation (GDPR) since past 25th May 2018 it is required to ask for consent and inform the individual about their actual situation and all the potential implications regarding the use of AI. Article 22 GDPR regulates this problem giving to each individual the right not to be subject to a solely automated decision producing legal or similarly significant effects. Originally taken this prohibition from the article 6a German Data Protection law, it obliges organisations to adopt measures to safeguard individuals when using solely automated decisions.

Artificial intelligence uses

Automated decision making (ADM) is the most common application of Artificial Intelligence (AI). Machine learning is a subfield that enables systems to learn without being explicitly programmed and the most common machine learning

---

1 Tweet of EDPS. Available at: https://twitter.com/EU_EDPS/status/1148654751850139649
uses for algorithms are profiling and automated individual decision making covering the latter a multitude of decision types, ranging from displaying search results, profiling or high-frequency trading⁴. All these acts must comply with GDPR requirements such as transparency, accountability or putting the subject in control of their data, but in practice most of the time these principles are violated, generating problems between the GDPR and AI.

Problems with data protection regulation

Despite their admirable objective at its core the drafting of article 22 of GDPR is very ambiguous when making a reference to AI, being required to solve several questions⁵. According to the professor Maja Brkan⁶ article 22 GDPR could produce on one hand scepticism towards biases and potentially false decisions that can be taken by automated means if they are not verified by humans, but on another hand by giving certain guarantees to each data subject, notably the right to human intervention, addresses concerns around the lack of ability of data subjects to influence decisions which are to an increasing extent taken by automated mean. AI processes always requires an extraordinary amount of data to learn and be able to make decisions, being data protection management a continuous danger in their activity. A preventive, but incomplete step, must be conduct an adequate Data Protection Impact Assessments following article 35 GDPR in order to ensure that actions has been taken adequately to manage any negative impact⁷. Some alarms were settled last year with the entry into force of the GDPR because several principles or issues that may create a conflict with AI as commonly practiced:

1. **Right to explanation**: The right to explain exists in the GDPR, albeit in a limited way concerning AI. Excluding the semantic question why this right

---


is designated as 'right to explanation'\textsuperscript{8}, data subjects have the right to understand the logic and the consequences of such logic to be able to challenge the legality of the decision. Important obstacles will be existent bias, discrimination and inaccuracies in data sets producing unreliable, discriminatory or unlawful algorithms. Also, each data subject must be able to know the potential the consequences of the ADM. GDPR recognizes the right to access the logic involved in automated decision making when the decision made by an algorithm has a significant impact on his life.

2. **Right to be forgotten**: Another key problem will be how to execute the right to be forgotten of the data subjects. How could it be possible to a machine forget the personal data that has been used to train an AI algorithm?\textsuperscript{9} It exists at least two different alternatives: retrain the models without the user data (expensive one) or find algorithm capable of "unlearn" certain specifics inputs without retraining over the entire dataset\textsuperscript{10}.

3. **Data portability**: this new right allows each data subject to access the personal data giving to a company and transfer it to another company. Exercising this right will provoke that AI companies would lose this data, being mandatory to transfer the information to another competitor that will use the new data to improve their AIs\textsuperscript{11}, supposing this right an potential competitive advantage to the best AI companies.

**Guidelines**

If we want an adequate implementation of the GDPR we must follow the interpretation contained in "Policy & investment recommendations for

\textsuperscript{8} Brkan, Maja (2019). Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond International Journal of Law and Information Technology, page 91.

\textsuperscript{9} Lacey, Elena (2019). The next big privacy hurdle? teaching AI to forget. Available at: https://www.wired.com/story/the-next-big-privacy-hurdle-teaching-ai-to-forget/

\textsuperscript{10} Hindi, Rand (2017). Will Artificial Intelligence Be Illegal in Europe Next Year?. Available at: https://www.entrepreneur.com/article/298394

\textsuperscript{11} Hindi, Rand (2017). Will Artificial Intelligence Be Illegal in Europe Next Year?. Available at: https://www.entrepreneur.com/article/298394
trustworthy AI"\(^\text{12}\) of the High-Level Expert Group on Artificial Intelligence enacted by High-Level Expert Group on AI \(^\text{13}\). In their Section 27.5 reminded that GDPR mandated transparency and explainability to the processing of personal data or the fact that ADM processes can also significantly affect individuals when the system is not fully automated or based on non-personal data. Also it is valuable the Guidelines on Automated Decision-making of the Article 29 Data Protection Working Party (now called European Data Protection Board)\(^\text{14}\). I must mention an interesting initiative is Project ExplAInto created by Information Commissioner’s Office, United Kingdom data protection authority, in collaboration with The Alan Turing Institute which aims to create practical guidance to assist organisations with explaining artificial intelligence decisions to the individuals affected\(^\text{15}\).

**Future challenges**

Cause AI is expected to be a major trigger in the fourth industrial revolution\(^\text{16}\), it will require a broader regulation taking into account the data protection principles. With the GDPR the European Union has placed itself at the forefront of protecting citizens' privacy. The new President of the European Commission Ursula von der Leyen\(^\text{17}\) sent a public communication to Didier Reyners, elected Commissioner of Justice, highlighting as “one of their main task will be contribute to the legislation on a coordinated approach on the human and

---


\(^{14}\) Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01) (2019). Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

\(^{15}\) Jones, Imogen (2019). It's time to AI-xplain. Available at: https://www.lexology.com/library/detail.aspx?g=b4ffcf80-9849-4d81-8d79-0e203b4b319d


ethical implications of artificial intelligence, ensuring that fundamental rights are fully protected in the digital age”. We can see as this statement highlights the importance of data protection, considered as a fundamental right, regarding to construct a new future in the European Union using AI techniques.

Bibliography

- Tweet of EDPS. Available at: https://twitter.com/EU_EDPS/status/1148654751850139649
- Lacey, Elena (2019). The next big privacy hurdle? teaching AI to forget. Available at: https://www.wired.com/story/the-next-big-privacy-hurdle-teaching-ai-to-forget/
- Hindi, Rand (2017). Will Artificial Intelligence Be Illegal in Europe Next Year?. Available at: https://www.entrepreneur.com/article/298394
- Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01) (2019). Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053