ISSN: 2977-0041

Mini Review

Journal of Material Sciences and Engineering Technology

The Role of GDPR in Artificial Intelligence, the Collection of Sensitive Personal Data and the Big Data

Christos P Beretas

Information Technology and Cyber Security, Innovative Knowledge Institute, Paris, France

Corresponding author
Christos P Beretas, Information Technology and Cyber Security, Innovative Knowledge Institute, Paris, France.

Received: February 22, 2023; **Accepted:** February 28, 2023; **Published:** March 04, 2023

ABSTRACT
Big Data and GDPR are two entities that do not go hand in hand. The systematic collection, storage, processing and analysis of data is a systematic process, which on the one hand is a necessity in artificial intelligence, but on the other hand it systematically limits personal data and human freedoms. Each country has different legislation or no legislation that defines and clarifies what personal information is and how this personal data is protected. The enthusiasm and passion for technological advancement should not affect people's personal lives. There are personal data which are of high importance to an individual which should not and is not ethical to be shared freely without any consent of the concerned individual as well as it is also unethical.

Keywords: GDPR, GDPR Violation, Surveillance, Personal Data, Ai, Artificial Intelligemce, Privacy, European Union, Big Data

Analysis

Without a doubt, artificial intelligence in today's era has made tremendous progress, it is all around us in various forms and automations. It is constantly evolving and the goal is to reach a level where it will be very close to human thought and logic and will be able to perform processes that were time-consuming, complex, or thought impossible until now. To implement all of the above, sophisticated algorithms and a large collection of data, known as **Big Data**, are required in order to extract the necessary information to be used later by the algorithms. All countries of the world do not apply the same policy to protect its citizens' personal data, some countries apply a strict policy and other countries do not apply any personal data protection policy. Big Data, and artificial intelligence unfortunately do not discriminate between countries and the laws applied by country, Big Data is collected from different sources, in different ways, and the way of processing varies. Given the above, it is impossible to apply the GDPR to limit and control the personal data of European citizens living in the European Union. Citizens of the European Union do not have the possibility to give its consent or not to its personal data collected and processed by third parties. It should be noted that the GDPR regulation is **opt-in / opt-out** which means that the European citizen should always give his/her consent to the **collection, storage and processing** of its personal data, he/she is also given the possibility to request the deletion of his/her personal data. This is a problem with Big Data, as there is no consent from the citizen. The European citizen, when he/she becomes aware of the leakage of its personal data, can do little to secure its personal data that has been leaked, he/she can report the leak to the competent authority for the protection of personal data, the citizen himself can contact the company / organization directly from which it realized the projection of its personal data, can contact non-governmental organizations that deal with the protection of personal data, or to proceed to third party organizations that may be available in each country. It is true that the citizen has minimal capabilities, and his/her personal data that has been published and that he/she does not know to the real extent exists in data centers around the world, the citizen detected a specific leak of personal data, does not mean this are the unique personal data that exist for the specific citizen, there may be other personal data that either have not yet been processed, or have not yet been identified by the algorithms.

In any case, the European citizen cannot object to the processing of its personal data, on the one hand, because he/she does not know the extent of the leak, and on the other hand, he/she does not know the reason behind the leak of his/her personal data, in order to ask for explanations and to ask for compensation for the moral damage to which he/she ia suffers. We conclude that, artificial intelligence must be used under the conditions, according to a single legislative framework, that it does not sacrifice the personal data, customs and manners, personal life

Citation: Christos P Beretas. The Role of GDPR in Artificial Intelligence, the Collection of Sensitive Personal Data and the Big Data. J Mat Sci Eng Technol. 2023. 1(1): 1-2. DOI: doi.org/10.61440/JMSET.2023.v1.05

and freedoms of the person, regardless of whether they are European citizens or not, whether or not there is a legislative framework for the protection of personal data in the country of collection, processing, analysis of information. In closing, emphasize should be given to the human right to employment, it is not right and ethical to cut jobs because of the use of artificial intelligence for the creation of automated production management systems, control of products and services, artificial intelligence should be used without abuse and always as an advisory agent in the choices of the human being as a chain of protection and control to reduce the chance of human error. An example of the use of artificial intelligence is **industry 4.0** which combines the human factor with artificial intelligence, providing an important security barrier [1-3].

References

1. Stephen Massey. Ultimate GDPR Practitioner Guide (2nd Edition): Demystifying Privacy & Data. Fox Red Risk; 2nd edition. 2020.
2. Christos Beretas. Security and Privacy in Data Networks. Research in Medical & Engineering Sciences. 2018 5: 469-478.
3. Christos Beretas Internet of Things and Privacy. Journal of Industrial Engineering and Safety. 2018. 1: 1-2.