

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

Christos P. Beretas,
Independent Researcher, France.

***Corresponding Author:** Christos P. Beretas, Independent Researcher, France.

Received: 21 March 2023; **Accepted:** 05 April 2022; **Published:** 10 April 2023.

Citation: Christos P. Beretas (2023), The Role of GDPR in Artificial Intelligence, the Collection of Sensitive Personal Data and the Big Data, International Journal of Reproductive Research 2(3): DOI: 10.58489/2836-2225/014

Copyright: © 2023 Christos P. Beretas. this is an open-access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Keywords: gdpr; gdpr violation; surveillance; personal data; AI; artificial intelligence; privacy; European union; big data

Summary

Without a doubt, artificial intelligence in today's era has made tremendous progress, it is all around us in various forms and automation. 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 their 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 the 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 their consent or not to the 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 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 his personal data, can do little to secure his personal data that has been leaked, he/she can report the leak to the competent

authority for the protection of personal data, and 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 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, European citizen cannot object to the processing of their 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 is 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 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, emphasis 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, and 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.

References

1. Beretas, C. P. (2023). The Continuous and Widespread Violation of GDPR In the Personal Communications of European Citizens, Disregarding Their Private Lives. *Eng OA*, 1(1), 01-04.
2. Beretas, C. (2018). Security and Privacy in Data Networks. *Research in Medical & Engineering Sciences*.
3. Beretas, C. (2018). Internet of Things and Privacy. *Journal of Industrial Engineering and Safety*, 1(1), 1-1.