Legal aspects of Big Data - GDPR

Nicolae Sfetcu

01.09.2019

Sfetcu, Nicolae, "Legal aspects of Big Data - GDPR", SetThings (September 1, 2019), URL = https://www.setthings.com/en/legal-aspects-of-big-data-gdpr/

Email: nicolae@sfetcu.com

A partial translation of:
Sfetcu, Nicolae, "Etica Big Data în cercetare", SetThings (6 iulie 2019), DOI: 10.13140/RG.2.2.27629.33761, MultiMedia Publishing (ed.), ISBN: 978-606-033-228-2, URL = https://www.setthings.com/ro/e-books/etica-big-data-in-cercetare/

The use of Big Data presents significant legal problems, especially in terms of data protection. The existing legal framework of the European Union based in particular on the Directive no. 46/95/EC and the General Regulation on the Protection of Personal Data provide adequate protection. But for Big Data, a comprehensive and global strategy is needed. The evolution over time was from the right to exclude others to the right to control their own data and, at present, to the rethinking of the right to (digital) identity.

The collection and aggregation of data in Big Data are not subject to data protection regulations, due to new perspectives on confidentiality, with the possibility of specific forms of discrimination.

In 2014, Podesta's report concluded that "big data analytics have the potential to eclipse longstanding civil rights protections in how personal information is used in housing, credit, employment, health, education, and the marketplace." (European Economic and Social Committee 2017) It follows that new specific ways of protecting citizens are needed, because the legal framework, although theoretically applicable, does not seem to provide adequate and full protection.

GDPR

The General Data Protection Regulation, "GDPR" (Regulation EU 2016/679) deals with data protection and privacy of persons in the European Union and the European Economic Area. It specifically addresses the export of personal data outside EU and EEA areas. The GDPR intends to simplify the regulatory environment by unifying the regulation within the EU. (European Parliament 2016)

GDPR applies in two cases for the processing of personal data: (a) access to goods or services for a fee by persons in the EU, or (b) monitoring their behavior within the EU. Thus, the regulation allows it to be extended to all Internet service providers, even if they are not established in the EU. More generally, GDPR applies to all large data aggregators, regardless of geographical or physical connections.

Stages of processing of personal data

The processing of personal data is defined in Article 4, paragraph 2, as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Big Data includes several personal data processing activities, each with its own specific rules:

1. data collection
2. data storage
3. data aggregation
4. data analysis and use of analysis results

Principles of data processing

Data processing is based on the following principles set out in Article 5 of the GDPR:

1. Legality, fairness and transparency: Users must be fully and properly informed regarding the privacy policy and be able to easily access their own data.
2. Purpose limitation: Data collectors must inform the data subject about the purposes of data collection, which can be further processed for those purposes only.
3. Data minimization: Only personal data relevant to the stated purposes will be collected.
4. Accuracy and updating: The data will be updated and rectified whenever required by the stated purpose. In the case of Big Data, the right of users to cancel or delete personal data is very important.
5. Limitation of storage: Data will be stored only during processing and subsequently destroyed. The duration of storage may be extended to the extent that the data are archived for public interest, scientific or historical research or statistical purposes.
6. Integrity and confidentiality: the data operator: Ensure adequate security for personal data through technical and organizational measures.

Privacy policy and transparency

In the case of data collection in order to complete a form, the principle of data minimization will be respected, only the relevant and strictly necessary data being requested. In the case of automatic

data collection, such as cookies, web monitoring or geolocation, the privacy policy must inform the user about this aspect.

Purposes of data processing

Anonymous and aggregate data can be processed to identify the behavior of certain categories of consumers. For this purpose, the data operator performs anonymization and then transfers them to a third party using them.

Design and implicit confidentiality

The concepts of privacy by design and implicit confidentiality were not explicitly included in EU regulations. But, according to art. 78 of the GDPR,

> "In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimizing the processing of personal data, pseudo-anonymizing personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations."

The (legal) paradox of Big Data

The use of Big Data implies at least one paradox: on the one hand, Big Data ensures maximum transparency but at the same time, there is no adequate transparency regarding the use of Big Data. Transparency is a fundamental issue because it influences the ability of a user to allow the disclosure of his information.

Bibliography

European Economic and Social Committee. 2017. "The Ethics of Big Data: Balancing Economic Benefits and Ethical Questions of Big Data in the EU Policy Context." European Economic

and Social Committee. February 22, 2017. https://www.eesc.europa.eu/en/our-work/publications-other-work/publications/ethics-big-data.

European Parliament. 2016. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA Relevance). OJ L.* Vol. 119. http://data.europa.eu/eli/reg/2016/679/oj/eng.