Fundamental rights implications of Big Data: privacy, data protection, non-discrimination, security and law-enforcement

2016/2225(INI) - 20/02/2017 - Committee report tabled for plenary, single reading

The Committee on Civil Liberties, Justice and Home Affairs adopted the own-initiative report by Ana GOMES (S&D, PT) on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement.

The prospects and opportunities of big data can only be fully tapped into by citizens, the public and private sectors, academia and the scientific community when public trust in these technologies is ensured by a strong enforcement of fundamental rights.

The report stressed that compliance with the existing data protection legislation, together with strong scientific and ethical standards, are key to establishing trust in and the reliability of big data solutions.

In order to enable citizens to have a better understanding of big data, Members suggested investing in digital literacy and awareness-raising about digital rights, privacy and data protection among citizens, including children.

Big data for commercial purposes and in the public sector: the report pointed out the need for much greater accountability and transparency with regard to data processing by the private and public sectors.

Data protection: Members stressed the fundamental role that the Commission, the European Data Protection Board, national data protection authorities and other independent supervisory authorities should play in the future to promote transparency, legal certainty and, more specifically, concrete standards that protect fundamental rights. They stressed that science, business and public communities should focus on research and innovation in the area of anonymisation and called for guidelines on how to properly anonymise data.

The private and public sectors are asked to make use of instruments provided for by the General Data Protection Regulation, such as codes of conduct and certification schemes, in order to seek greater certainty over their specific obligations under Union law.

Security: the report stressed the need for a genuine cooperation between the public and private sectors, the law enforcement authorities and the independent supervisory data protection authorities to in order to tackle threats to security, security breaches, unauthorised access to data and unlawful surveillance.

The report suggested encouraging the use of end-to-end encryption and, where necessary, mandated in accordance with the principle of data protection by design. It called for the use of privacy by design and default.

Non- discrimination: Members called for all measures possible to be taken to minimise algorithmic discrimination and bias and to develop a common ethical framework for the transparent processing of personal data and automated decision-making. This common framework may guide data usage and the ongoing enforcement of Union law.

Moreover, the use of big data for scientific purposes should be conducted with due regard for the fundamental values and in compliance with current EU data protection legislation.

Big data for law enforcement purposes: Members reminded all law enforcement actors that use data processing and analytics that Directive (EU) 2016/680 governing the processing of personal data by Member States for law enforcement purposes. They welcomed the publication of guidelines, recommendations and best practices in order to further specify the criteria and conditions for decisions based on profiling and the use of big data for law enforcement purposes.

Lastly, the report underlined the absolute need to protect law enforcement databases from security breaches and unlawful access. It called for maximum caution to be taken in order to prevent unlawful discrimination and the targeting of certain individuals or groups of people when processing and analysing data.