Procedure file

Basic information

INI - Own-initiative procedure	2016/2225(INI)	Procedure completed
Fundamental rights implications of Big Data: privacy, data protection, non-discrimination, security and law-enforcement Subject 1.10 Fundamental rights in the EU, Charter 1.20.09 Protection of privacy and data protection 3.30.06 Information and communication technologies, digital technologies		

Key players

European Parliament	Committee responsible	Rapporteur	Appointed
	LIBE Civil Liberties, Justice and Home Affairs		07/03/2016
		S&D GOMES Ana	
		Shadow rapporteur	
		epp VOSS Axel	
		ECR ŠKRIPEK Branislav	
		PETERSEN Morten	
		ALBRECHT Jan Philipp	
	Committee for opinion	Rapporteur for opinion	Appointed
	ITRE Industry, Research and Energy	The committee decided not to give an opinion.	
European Commission	Commission DG	Commissioner	
	Justice and Consumers	JOUROVÁ Věra	

Key events

15/09/2016	Committee referral announced in Parliament		
09/02/2017	Vote in committee		
20/02/2017	Committee report tabled for plenary	A8-0044/2017	Summary
13/03/2017	Debate in Parliament		
14/03/2017	Results of vote in Parliament		
14/03/2017	Decision by Parliament	T8-0076/2017	Summary
14/03/2017	End of procedure in Parliament		

Technical information

Procedure reference	2016/2225(INI)
Procedure type	INI - Own-initiative procedure
Procedure subtype	Initiative
Legal basis	Rules of Procedure EP 54
Other legal basis	Rules of Procedure EP 159
Stage reached in procedure	Procedure completed
Committee dossier	LIBE/8/07753

Documentation gateway

Committee draft report		PE592.279	19/10/2016	EP	
Amendments tabled in committee		PE595.750	19/12/2016	EP	
Committee report tabled for plenary, single reading		A8-0044/2017	20/02/2017	EP	Summary
Text adopted by Parliament, single reading		T8-0076/2017	14/03/2017	EP	Summary
Commission response to text adopted in plenary		SP(2017)390	22/08/2017	EC	

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

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.

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

The European Parliament adopted by 561 votes to 71, with 49 abstentions, a resolution on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement.

Big data has the potential for citizens, academia, the scientific community and the public and private sectors, but also entails significant risks, namely with regard to the protection of fundamental rights, the right to privacy, data protection, non-discrimination and data security.

Parliament 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 resolution pointed out the need for much greater accountability and transparency with regard to data processing by the private and public sectors.

Data protection: Members underlined the importance of:

- promoting transparency and due process, legal certainty in general and, more specifically, concrete standards that protect fundamental rights and guarantees associated with the use of data processing and analytics by the private and public sector;
- closer collaboration among regulators of conduct in the digital environment;
- focusing on research and innovation in the area of anonymisation and preparing guidelines on how to properly anonymise data in order to avoid future abuses of these measures and to monitor practices;
- ensuring that data-driven technologies do not limit or discriminate access to a pluralistic media environment, but rather foster media freedom and pluralism.

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: in order to address the most pressing risks associated with data processing activities, Parliament:

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

Non-discrimination: big data may result not only in infringements of the fundamental rights of individuals, but also in differential treatment of and indirect discrimination against groups of people with similar characteristics, particularly with regard to fairness and equality of opportunities for access to education and employment.

Parliament 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: the trust of citizens in digital services can be seriously undermined by government mass surveillance activities.

Stressing the importance of compliance with Directive (EU) 2016/680, Parliament 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 resolution 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.