DRAFT REPORT

on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement (2016/2225(INI))

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Ana Gomes
<table>
<thead>
<tr>
<th>CONTENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Page</td>
</tr>
<tr>
<td>MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION ........................................ 3</td>
</tr>
</tbody>
</table>
MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION

on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement (2016/2225(INI))

The European Parliament,

– having regard to Article 16 of the Treaty on the Functioning of the European Union,

– having regard to Articles 1, 7, 8, 11, 14, 21, 47 and 52 of the Charter of Fundamental Rights of the European Union,

– having regard to 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 - GDPR)¹, and to Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA²,

– having regard to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data of 28 January 1981 (ETS 108) and its Additional Protocol of 8 January 2001 (ETS 181)³,

– having regard to Recommendation CM/Rec(2010)13 of the Committee of Ministers of the Council of Europe to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling of 23 November 2010⁴,

– having regard to Opinion 7/2015 of the European Data Protection Supervisor of 19 November 2015 entitled ‘Meeting the challenges of big data; A call for transparency, user control, data protection by design and accountability’⁵,

– having regard to the statement of the Article 29 Working Party on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU of 16 September 2014⁶,

– having regard to Rule 52 of its Rules of Procedure,

– having regard to the report of the Committee on Civil Liberties, Justice and Home Affairs and the opinion of the Committee on Industry, Research and Energy (A8-
 whereas big data refers to the recurring accumulation of large amounts of data, including personal data, from a variety of sources, which are subject to automatic processing by computer algorithms and advanced data-processing techniques in order to generate certain correlations, trends and patterns (big data analytics);

 B. whereas the progress of communication technologies and the ubiquitous use of electronic devices, monitoring gadgets, social media, web interactions and networks, including devices which communicate information without human interference, have led to the development of massive, ever-growing data sets which, through advanced processing techniques and analytics, provide unprecedented insight into human behaviour and our societies;

 C. whereas corporations, governments and organisations have taken advantage of such data sets and big data analytics to foster competitiveness, innovation, market prediction, targeted advertising, scientific research and policy making in the field of transportation, ‘smart cities’, law enforcement, transparency, public health and disaster response;

 D. whereas big data has the potential to bring undeniable benefits and opportunities for citizens, businesses and governments, but also entails significant risks, namely with regard to the protection of fundamental rights as guaranteed by the EU Charter and Union law;

 E. whereas the pervasiveness of sensors, extensive routine data production and contemporary data-processing activities are characterised by a high degree of opacity;

 F. whereas biased algorithms and other analytical tools, low quality of data, spurious correlations, errors, the underestimation of legal, social and ethical implications and the marginalisation of the role of humans in these processes can trigger flawed decision-making procedures;

 G. whereas the proliferation of data processing and analytics, the multitude of actors involved in collecting, retaining, processing and sharing data and the combination of large data sets containing personal data from a variety of sources, retained for unlimited amounts of time, have all created great uncertainty for both citizens and businesses over the specific requirements for compliance with general data-protection principles;

 **General considerations**

 1. Emphasises that information revealed by big data analysis is only as reliable as the underlying data permits, and that strong scientific and ethical standards are therefore needed for judging the results of such analysis and its predictive algorithms;

 2. Stresses that the prospects and opportunities of big data can only be fully enjoyed by citizens, corporations, governments and institutions when public trust in these technologies is ensured by strong enforcement of fundamental rights and legal certainty for all actors involved;
Big data for commercial purposes and in the public sector

Privacy and data protection

3. Points out that Union law for the protection of privacy and personal data, as well as the rights to equality and non-discrimination, are applicable to data processing even when that processing is preceded by pseudonymisation and anonymisation techniques, insofar as there are risks of re-identification, or, in any case, when use of non-personal data might impact on individuals’ private lives or other rights and freedoms;

4. Takes the view that transparency, fairness, accountability and control over personal data are core values through which specific rights and obligations are derived, and which should guide the action of corporations, public authorities and other actors that use data to frame their decision-making procedures; emphasises the need for much greater transparency with regard to data processing and analytics by businesses;

5. Highlights the fundamental role that the Commission, the European Data Protection Board and other independent supervisory authorities should play in the coming years and decades to promote legal certainty concerning concrete standards protecting fundamental rights and guarantees associated with the use of data processing and analytics;

6. Takes the view that anonymisation techniques should comprise technical measures and contractual obligations which ensure non-re-identification; calls on corporations to regularly review such risks in light of new technologies and to document the appropriateness of measures adopted, allowing independent supervisory authorities to monitor practices and provide recommendations;

7. Urges corporations and other data controllers to make use of instruments provided for by the GDPR, such as codes of conduct and certification schemes, to seek greater certainty over their specific obligations under Union law and to bring their practices and activities into compliance with the appropriate Union legal standards and safeguards;

Security

8. Acknowledges that data loss and theft, infection by malware, unauthorised access to data and unlawful surveillance are some of the most pressing risks associated with contemporary data processing activities, such as big data techniques; believes that tackling such threats requires genuine and concerted cooperation between the private sector, governments, law enforcement authorities and independent supervisory authorities;

Non-discrimination

9. Calls on the Union and the Member States to identify and minimise algorithmic discrimination and bias and to develop a strong and common ethics framework for the processing of personal data and automated decision-making;
Big data for law enforcement purposes

Privacy and data protection

10. Encourages all law enforcement actors that use data processing and analytics to ensure appropriate human intervention throughout the various stages of the processing and analysis of data, especially when decisions may carry high risks for individuals;

11. Stresses, in particular, the importance of carrying out prior impact assessments that take account of ethical concerns in order to assess the inclusiveness, accuracy and quality of the data, and to ensure that individuals targeted by the decisions and/or actors involved in the decision-making processes are able to challenge the analysis, patterns and correlations and to prevent any harmful effects on certain groups of individuals;

Security

12. Underlines the absolute need to protect law enforcement databases from data loss and theft, infection by malware and unauthorised access to data by non-authorised persons; believes that tackling such concerns requires genuine, concerted cooperation between law enforcement authorities and independent supervisory authorities;

Non-discrimination

13. Warns that, owing to the intrusiveness of decisions and measures taken by law enforcement authorities in citizens’ lives and rights, maximum caution is necessary to avoid unlawful discrimination and the targeting of certain population groups, especially marginalised groups and ethnic and racial minorities;

14. Calls on the Member States’ law enforcement authorities that make use of data analytics to uphold the highest standards of ethics in the analysis of data and to ensure human intervention and accountability throughout the different stages of decision-making, not only to assess the representativeness, accuracy and quality of the data, but also to assess the appropriateness of each decision to be taken on the basis of that information;

15. Instructs its President to forward this resolution to the Council and the Commission.