European Parliament
2014-2019

Committee on Civil Liberties, Justice and Home Affairs

2015/2147(INI)

01.12.2015

OPINION

of the Committee on Civil Liberties, Justice and Home Affairs

for the Committee on Industry, Research and Energy and the Committee on the Internal Market and Consumer Protection

on Towards a Digital Single Market Act
(2015/2147(INI))

Rapporteur (*): Michał Boni

(*) Associated committee – Rule 54 of the Rules of Procedure

SUGGESTIONS

The Committee on Civil Liberties, Justice and Home Affairs calls on the Committee on Industry, Research and Energy and the Committee on the Internal Market and Consumer Protection, as the committees responsible, to incorporate the following suggestions into their motion for a resolution:

1. Stresses the need for compliance with fundamental rights, in particular data protection legislation, of all initiatives developed under the Digital Single Market Strategy, while recognising the strategy's added value to the EU economy; underlines the fact that respect for fundamental rights, in particular privacy and the protection of personal data, are key elements in building citizens' trust and security, which are necessary for the development of the data-driven economy to embrace the potential of the digital sector and should thus be considered as creating opportunities and a competitive advantage; stresses the need for cooperation between technologies, business and public authorities to ensure compliance with the applicable EU legislation; recalls the importance of swift adoption of both the General Data Protection Regulation and the Data Protection Directive, in the interest of both data subjects and businesses; calls for the revision of the ePrivacy Directive to ensure the consistency of provisions with the data protection package by the time of the entry into force of the package;

3.3.2. Combating illegal content on the internet

2. Calls on the Commission to advance policies and a legal framework to tackle cybercrime and illegal content and materials on the internet, including hate speech, that will be in full compliance with fundamental rights as set out in the Charter of Fundamental Rights of the European Union, in particular the right to freedom of expression and information, with existing EU or Member State legislation and with the principles of necessity, proportionality, due legal process and the rule of law; considers that, in order to achieve that goal, it is necessary to:
   – provide consistent and efficient law enforcement tools for European and national police agencies and law enforcement authorities;
   – provide clear guidelines on how to tackle illegal content online, including hate speech;
   – support public-private partnerships and dialogue between public and private entities, in compliance with existing EU legislation;
   – clarify the role of intermediaries and online platforms with respect to the Charter of Fundamental Rights of the European Union;
   – ensure that the creation within Europol of the European Union Internet Referral Unit (EU IRU) is founded on a legal basis that is appropriate for its activities;
   – ensure special measures to combat the sexual exploitation of children online and effective cooperation between all stakeholders to guarantee the rights and protection of children on the internet and encourage initiatives that strive to make the internet safe for children, and
   – cooperate with the relevant stakeholders in promoting education and awareness-raising campaigns;

3. Recalls that, under Article 12 of the Directive on electronic commerce (2000/31/EC), 'where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the

provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider does not initiate the transmission, does not select the receiver of the transmission, and does not select or modify the information contained in the transmission';

3.4. Reinforcing trust and security in digital services and in the handling of personal data

4. Highlights the fact that the fast-growing number of attacks on networks and acts of cybercrime calls for a harmonised response from the EU and its Member States with a view to ensuring a high level of network and information security; believes that providing security on the internet entails the protection of networks and critical infrastructure, ensuring the ability of law enforcement agencies to fight crime, including terrorism, violent radicalisation and sexual abuse and the sexual exploitation of children online, and use of data that are strictly necessary to fight crime online and offline; stresses that security, thus defined, together with protection of fundamental rights in cyberspace, is crucial to reinforcing trust in digital services and is therefore a necessary basis for establishing a competitive digital single market;

5. Calls for the final adoption of the Network and Information Security (NIS) Directive with a view to providing a consistent regulatory framework to secure strategic and operational cybersecurity at both EU and national level, which requires closer cooperation with national authorities and EU agencies, while ensuring the protection of EU fundamental rights, in particular privacy and data protection for businesses, public administrations and data subjects;

6. Recalls that tools such as encryption are useful to citizens and businesses as a means of ensuring privacy and at least a basic level of communications security; condemns the fact that it can also be used for criminal purposes;

7. Welcomes the establishment of a European Cybercrime Centre (EC3) within Europol which contributes to faster reactions in the event of cyber-attacks; calls for a legislative proposal to reinforce EC3's mandate, and calls for swift transposition of Directive 2013/40/EU of 12 August 2013 on attacks against information systems, which is also aimed at improving operational cooperation between Member States' national law enforcement services and the relevant EU agencies (Eurojust, Europol and EC3, and ENISA);

8. Welcomes the Commission's initiative to establish a public-private partnership (PPP) on cybersecurity; underlines the need for the cooperation and involvement of businesses and the introduction of the security-by-design concept; supports the sharing of Member States' good practice in PPPs in this area; regrets, in this connection, the closing of the European Public-Private Partnership for Resilience (EP3R);

9. Notes that the revelations of electronic mass surveillance have shown the need to regain the citizens' trust in the privacy, safety and security of digital services, and underlines, in this connection, the need for strict compliance with existing data protection legislation and respect for fundamental rights, when processing personal data for commercial or law enforcement purposes; recalls, in this context, the importance of existing tools such as mutual legal assistance treaties (MLATs), which respect the rule of law and decrease the

risk of improper access to data that is stored in foreign territory;

10. Reiterates that, under Article 15(1) of the Directive on electronic commerce (2000/31/EC), 'Member States shall not impose a general obligation on providers' of transmission, storage and hosting services 'to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity'; reiterates, in particular, that the Court of Justice of the European Union, in its Judgments C-360/10 and C-70/10, rejected measures for the 'active monitoring' of almost all users of the services concerned (internet access providers in one case, a social network in the other) and specified that any injunction requiring a hosting services provider to undertake general monitoring should be precluded;

4.1.Building a data economy

11. Considers that big data, cloud services, the Internet of Things, research and innovation are key to economic development and need a coherent approach throughout EU legislation; believes that compliance with data protection legislation and effective privacy safeguards and security safeguards as set in the General Data Protection Regulation, including special provisions regarding children as vulnerable consumers, are crucial for building trust for citizens and consumers in the data-driven economy sector; stresses the need to raise awareness of the role of data and the meaning of data-sharing for consumers, as regards their fundamental rights and within the economy, and to lay down rules on data ownership and citizens' control over their personal data; underlines the role of personalisation of services and products that should be developed in compliance with data protection requirements; calls for the promotion of privacy by default and by design, which could also have positive impact on innovation and economic growth; stresses the need to ensure a non-discriminatory approach to all data processing; underlines the importance of a risk-based approach, which helps avoid any unnecessary administrative burden and provides legal certainty, as in the General Data Protection Regulation, especially for SMEs and start-ups, as well as democratic oversight and constant monitoring by public authorities; stresses that personal data need special protection and recognises that putting in place additional safeguards, such as pseudonymisation or anonymisation, can enhance protection where personal data are used by big data applications and online service providers;

4.2. Boosting competitiveness through interoperability and standardisation

12. Stresses that any processing of personal data through interoperability-based solutions, i.e. operated by the ISA² programme, must comply with the requirements of EU data protection laws; calls for improved cooperation in order to establish common, global standards for the data-driven economy, which should prioritise security, respect for privacy and data protection; stresses the importance of citizens' right to data portability;

4.3.2. E-government

13. Supports the digitalisation of public services in Europe, the development of e-government, e-democracy and open data policies, access to and reuse of public documents based on transparency and the existing EU legal framework, and high data protection standards as proposed in the Data Protection Reform package and fully in line with the Charter of Fundamental Rights; recalls that e-government contributes to genuine participation,

consultation, and a more transparent, accountable and efficient public administration; stresses, in this connection, the importance of exchanges of best practice between all the relevant stakeholders;

14. Emphasises, while supporting the development of e-government, including the promotion of the once-only principle, that all e-government initiatives must comply with the requirements and principles of the data protection reform package and that a high level of security must be ensured for these initiatives to protect the citizens' data provided to public institutions;

5.2. International dimension

15. Recognises the global nature of the data economy; recalls that the creation of the digital single market is dependent on the free flow of data within and outside the European Union; calls, therefore, for steps to be taken by the EU and its Member States in cooperation with third countries to ensure high standards of data protection and safe international data transfers, in compliance with the General Data Protection Regulation and the existing EU case law, when pursuing cooperation with third countries within the Digital Single Market Strategy.

RESULT OF FINAL VOTE IN COMMMITTEE ASKED FOR OPINION

Date adopted	30.11.2015
Result of final vote	+: 49 –: 1 0: 2
Members present for the final vote	Jan Philipp Albrecht, Michał Boni, Ignazio Corrao, Agustín Díaz de Mera García Consuegra, Frank Engel, Kinga Gál, Ana Gomes, Nathalie Griesbeck, Sylvie Guillaume, Jussi Halla-aho, Monika Hohlmeier, Brice Hortefeux, Sophia in ‘t Veld, Sylvia-Yvonne Kaufmann, Barbara Kudrycka, Marju Lauristin, Juan Fernando López Aguilar, Roberta Metsola, Louis Michel, Claude Moraes, Alessandra Mussolini, József Nagy, Soraya Post, Judith Sargentini, Birgit Sippel, Branislav Škripek, Csaba Sógor, Helga Stevens, Bodil Valero, Marie-Christine Vergiat, Harald Vilimsky, Udo Voigt, Beatrix von Storch, Josef Weidenholzer, Cecilia Wikström, Kristina Winberg, Tomáš Zdechovský
Substitutes present for the final vote	Carlos Coelho, Anna Hedh, Teresa Jiménez-Becerril Barrio, Marek Jurek, Ska Keller, Miltiadis Kyrkos, Jeroen Lenaers, Nuno Melo, Emilian Pavel, Morten Helveg Petersen, Barbara Spinelli, Axel Voss
Substitutes under Rule 200(2) present for the final vote	Jens Geier, Gabriele Preuß, Marco Zanni