EUROPEAN PARLIAMENT 2009 - 2014

Committee on Civil Liberties, Justice and Home Affairs

2013/2063(INI)

19.9.2013

OPINION

of the Committee on Civil Liberties, Justice and Home Affairs

for the Committee on Industry, Research and Energy

on unleashing the potential of cloud computing in Europe
(2013/2063(INI))

Rapporteur(*): Judith Sargentini

(*) Associated committee – Rule 50 of the Rules of Procedure

SUGGESTIONS

The Committee on Civil Liberties, Justice and Home Affairs calls on the Committee on Industry, Research and Energy, as the committee responsible, to incorporate the following suggestions in its motion for a resolution:

1. Reiterates that alongside the potential and benefits of 'cloud computing' for businesses, citizens, the public sector and the environment, in particular in terms of cost reduction, it entails significant risks and challenges, particularly for fundamental rights (including privacy and data protection) and by increasing impact in case of disruptions, whether they are caused by malfunction, malpractice, criminal action or hostile action by another country;

2. Takes the view that access to a safe internet is a fundamental right of every citizen and that 'cloud computing' will continue to play an important role in this aspect; reiterates, therefore, its call on the Commission and the Council unequivocally to recognise digital freedoms as fundamental rights and as indispensable prerequisites for enjoying universal human rights;

3. Reiterates that, as a general rule, the level of data protection in a 'cloud computing' environment must not be inferior to that required in any other data-processing context;

4. Stresses that Union data protection law, since it is technologically neutral, already now fully applies to cloud computing services operating in the EU and must, therefore, be fully respected; stresses that the opinion of the Working Party of the Article 29 (WP29) on Cloud Computing1 should be taken into account as it provides clear guidance for the application of Union data protection law principles and rules to cloud services, such as the concepts of controller/processor, purpose limitation and proportionality, integrity and data security, the use of subcontractors, allocation of responsibilities, data breaches and international transfers; underlines the need to close any gaps in the protection as regards cloud computing in the ongoing review of the Union data protection legal framework based on further guidance by the European Data Protection Supervisor (EDPS) and the WP29; considers that not all sensitive information is personal data, and therefore urges the Commission to propose guidelines to protect non-personal sensitive data in a cloud context, particularly in the case of government data and of data from organisations such as banks, insurance companies, pension funds, schools and hospitals;

5. Recalls that where a cloud provider uses the data for a purpose other than that agreed on in the service agreement, or communicates data or uses it in a way contrary to the terms of the contract, he should be considered data controller and should be held liable for the infringements and breaches incurred;

6. Stresses that cloud services agreements must set out, in a clear and transparent manner, the duties and rights of the parties concerning data processing activities by cloud providers; the contractual arrangements shall not entail a waiver of the safeguards, rights and protections afforded by Union data protection law; urges the Commission to come

[1] Opinion 5/2012, WP 196, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#h2-1

forward with proposals to restore the balance between cloud service providers and their customers as regards the terms and conditions used by cloud services, including provisions;

– ensuring protection against arbitrary cancellation of services and deletion of data;

– guaranteeing a reasonable chance for customer to recover stored data in case of cancellation of service and/or removal of data;

– providing clear guidelines for cloud providers to facilitate the easy migration of their customers to other services;

7. Highlights that the role of the cloud service provider under current Union legislation needs to be determined on a case-by-case basis, as providers can be both data processors and data controllers; calls for the terms and conditions for all users to be improved through the development of international best practice models for contracts and through the clarification of where the service provider stores data and under which area of law within the EU;

8. Highlights that particular attention must be given to situations in which the imbalance in the contractual situation between the customer and the cloud provider leads the customer to enter into contractual arrangements imposing standard services and a contract to be signed in which the provider defines the purposes, conditions and means of the processing1; stresses that, in such circumstances, the cloud provider should be considered ‘data controller’ and become jointly liable with the customer;

9. Stresses that the use of cloud services by public authorities, including by law enforcement authorities and EU institutions, requires special consideration and coordination between the Member States; recalls that data integrity and security must be guaranteed and unauthorised access, including by foreign governments and their intelligence services without a legal basis under Union or Member State law, prevented; stresses that this also applies to the specific processing activities of certain essential non-governmental services, in particular the processing of specific categories of personal data, such as banks, insurance companies, pension funds, schools and hospitals; urges the Commission to issue guidelines for these organisations to follow when using cloud services to process, transmit or store their data, including the adoption of open standards to prevent vendor lock-in, and a preference for open source software to improve transparency and accountability of the services used; stresses, furthermore, that all of the aforementioned is of particular importance if data is being transferred (outside the European Union between different jurisdictions); takes the view, therefore, that public authorities, as well as non-governmental services and the private sector, should, as far as possible, rely on EU cloud providers when processing sensitive data and information until satisfactory global rules on data protection have been introduced, ensuring the security of sensitive data, and of data bases, held by public entities;

10. Recalls its serious concern about the recent unveiling of US National Security Agency

[1] Particularly in the case of consumers and SMEs using cloud services.

surveillance programmes, and of similar programmes operated by intelligence agencies in various Member States, in the recognition that, should the information available up to now be confirmed, these programmes entail a serious violation of the fundamental right of EU citizens and residents to privacy and data protection, as well as of the right to private and family life, the confidentiality of communications, the presumption of innocence, freedom of expression, freedom of information, and the freedom to conduct business;

11. Reiterates its serious concerns about the compulsory direct disclosure of EU personal data and information, processed under cloud agreements, to third country authorities by cloud providers subject to third country laws or using storage servers located in third countries, and about direct remote access to personal data and information processed by third-country law enforcement authorities and intelligence services;

12. Regrets that such access is usually attained by means of direct enforcement by third countries authorities of their own legal rules, without recourse to international instruments established for legal cooperation such as mutual legal assistance (MLA) agreements or other forms of judicial cooperation;

13. Stresses that such practices raise questions of trust as regards non-EU cloud and online service providers, and as regards third countries that do not rely on international instruments for legal and judicial cooperation;

14. Expects the Commission and the Council to take such measures as are necessary to solve this situation and to ensure the respect of the fundamental rights of EU citizens;

15. Recalls that all companies providing services in the EU must, without exception, comply with EU law and are liable for any breaches;

16. Stresses that cloud services that fall under third country jurisdiction should provide users located in the EU with a clear and distinguishable warning of the possibility that their personal data may be subject to intelligence and law enforcement surveillance by third country authorities under secret orders or injunctions, followed, where applicable, by a request for the data subject's explicit consent for the processing of personal data;

17. Urges the Commission, when negotiating international agreements that involve the processing of personal data, to take particular note of the risks and challenges that cloud computing poses to fundamental rights, in particular – but not exclusively – the right to private life and to the protection of personal data, as laid down in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union; urges, furthermore, the Commission to take note of the negotiating partner's domestic rules governing the access of law enforcement and intelligence agencies to personal data processed through cloud computing service, in particular by demanding that such access for law enforcement and intelligence authorities only be granted with full respect for the due process of law and on an unambiguous legal basis, as well as the requirement that the exact conditions of access, the purpose of gaining such access, the security measures put in place when handing over data and the rights of the individual, as well as the rules for supervision and for an effective redress mechanism, be specified;

18. Stresses its serious concerns about the work carried out within the Council of Europe's

Cybercrime Convention Committee with a view to developing an additional protocol on the interpretation of Article 32 of the Convention on Cybercrime of 23 November 2001 on 'trans-border access to stored computer data with consent or where publicly available'1 in order to 'facilitate its effective use and implementation in the light of legal, policy and technological developments'; calls on the Commission and the Member States, in view of the forthcoming consideration by the Committee of Ministers of the Council of Europe, to ensure the compatibility of the provision of Article 32 of the Convention on Cybercrime, and its interpretation in the Member States, with fundamental rights, including data protection and, in particular, the provisions on trans-border flows of personal data, as enshrined in the EU Charter of Fundamental Rights, the EU data protection *acquis*, the European Convention of Human Rights and the Council of Europe Convention on the Protection of Individuals with Regard to Automatic Processing ('Convention 108'), which are legally binding upon the Member States; calls on the Commission and the Member States to reject firmly any measure that would put the application of these rights at risk; is alarmed by the fact that should such an additional protocol be endorsed, its implementation could result in unfettered remote access by law enforcement authorities on servers and computer systems located in other jurisdictions, without recourse to MLA agreements and other instruments of judicial cooperation put in place to guarantee the fundamental rights of the individual, including data protection and due process;

19. Underlines that particular attention must be paid to small and medium-sized enterprises which increasingly rely on 'cloud computing' technology when processing personal data, and which may not always have the resources or the expertise to address security challenges adequately;

20. Stresses that the qualification of data controller or processor needs to be appropriately reflected by the actual level of control it has over the means of processing, in order that the responsibilities for the protection of personal data with the use of cloud computing are clearly allocated;

21. Underlines the importance of digital literacy among all citizens, and urges the Member States to develop concepts of how to promote the safe use of internet services, including 'cloud computing';

22. Stresses that all the principles laid down in EU data protection law, such as fairness and lawfulness, purpose limitation, proportionality, accuracy and limited data retention periods, must be taken fully into account by cloud computing service providers when processing personal data;

23. Underlines the importance of having effective, proportionate and dissuasive administrative sanctions that may be imposed on 'cloud computing' services that do not comply with EU data protection standards;

24. Stresses that, in order to define the most appropriate safeguards to implement, the data protection impact of each cloud computing service must be assessed on an ad hoc basis;

[1] 1http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/TCY(2013)14transb_elements_protocol_V2.pdf
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp

25. Stresses that a European cloud service provider should always act in conformity with EU data protection law, even if this conflicts with instructions by a client or controller established in a third country, or when the data subjects concerned are (solely) residents of third countries;

26. Stresses the need to address the challenges raised by cloud computing at an international level, in particular as regards government intelligence surveillance and necessary safeguards;

27. Stresses that EU citizens subject to intelligence surveillance by third country authorities should benefit from at least the same safeguards and remedies as are available to citizens of the third country concerned;

28. Regrets the approach in the Commission's communication whereby it fails to mention the risks and challenges attached to cloud computing, and urges the Commission to continue its work on cloud computing by developing a more holistic communication on cloud computing that takes into account the interests of all stakeholders, and that contains, alongside a standard reference to the protection of fundamental rights and compliance with data protection requirements, at least the following:

– guidelines to ensure full compliance with the EU's fundamental rights and data protection obligations;

– limitative conditions under which cloud data may or may not be accessed for law enforcement purposes, in compliance with the EU Charter of Fundamental Rights and with EU law;

– safeguards against illegal access by foreign and domestic entities, for instance by amending procurement requirements and applying Council Regulation (EC) No 2271/96[1] to counteract foreign laws that may result in massive illegal transfers of the cloud data of EU citizens and residents;

– proposals to guarantee net neutrality and service neutrality in order to prevent commercially motivated discrimination against specific cloud services;

– proposals to guarantee that access to legal content will not be harmed by actions against illegal content;

– proposals on how to define the 'transfer' of personal data and on how to update standard contractual clauses that are tailored to the cloud environment, as 'cloud computing' often involves massive flows of data from cloud clients to cloud providers' servers and data centres, involving many different parties and crossing borders between EU and non-EU countries;

– measures to address the existing imbalance in the cloud services market between service providers and most of the users of their services;

[1] Council Regulation (EC) No 2271/96 of 22 November 1996 protecting against the effects of the extra-territorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom (OJ L 309, 29.11.1996, p. 1 - 6; URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996R2271:EN:HTML)

– measures promoting research on how current EU legislative frameworks and international agreements fit particular cloud computing services scenarios, measuring both the economic and the environmental impact of cloud computing, as few studies have yet been made on these aspects.

RESULT OF FINAL VOTE IN COMMITTEE

Date adopted	18.9.2013
Result of final vote	+: 43 –: 3 0: 1
Members present for the final vote	Jan Philipp Albrecht, Roberta Angelilli, Edit Bauer, Rita Borsellino, Emine Bozkurt, Arkadiusz Tomasz Bratkowski, Salvatore Caronna, Philip Claeys, Carlos Coelho, Ioan Enciu, Cornelia Ernst, Tanja Fajon, Hélène Flautre, Kinga Gál, Kinga Göncz, Sylvie Guillaume, Ágnes Hankiss, Anna Hedh, Salvatore Iacolino, Sophia in ‘t Veld, Lívia Járóka, Timothy Kirkhope, Juan Fernando López Aguilar, Svetoslav Hristov Malinov, Clemente Mastella, Véronique Mathieu Houillon, Claude Moraes, Georgios Papanikolaou, Carmen Romero López, Judith Sargentini, Birgit Sippel, Csaba Sógor, Renate Sommer, Rui Tavares, Nils Torvalds, Wim van de Camp, Axel Voss, Renate Weber, Josef Weidenholzer, Tatjana Ždanoka, Auke Zijlstra
Substitute(s) present for the final vote	Alexander Alvaro, Cornelis de Jong, Mariya Gabriel, Marian-Jean Marinescu, Salvador Sedó i Alabart, Janusz Wojciechowski
Substitute(s) under Rule 187(2) present for the final vote	Nuno Teixeira