Resolution on the follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens

2015/2635(RSP) - 29/10/2015 - Text adopted by Parliament, single reading

The European Parliament adopted by 342 votes to 274 with 29 abstentions a resolution tabled by the Committee on Civil Liberties, Justice and Home Affairs on the follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens.

Parliament referred to its resolution 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens fundamental rights and on transatlantic cooperation in Justice and Home Affairs. It stated that it was highly disappointed by the overall lack of sense of urgency and willingness shown by most Member States and the EU institutions in terms of seriously addressing the issues raised in the resolution and implementing the concrete recommendations contained therein, as well as by the lack of transparency towards or dialogue with Parliament.

Members considered the Commissions reaction so far to the resolution to be highly inadequate and they called for action by the Commission by December 2015 at the latest, reserving the right to bring an action for failure to act or to place certain budgetary resources for the Commission in a reserve until all the recommendations had been properly addressed.

By 285 votes to 281, Parliament decided to call on EU member states to drop any criminal charges against Edward Snowden, grant him protection and consequently prevent extradition or rendition by third parties, in recognition of his status as whistle-blower and international human rights defender.

Parliament was concerned at some of the recent laws in some Member States that extend surveillance capabilities of intelligence bodies, and it referred to cases in France, the United Kingdom, the Netherlands, and interceptions in Germany by the BND.

Safe Harbour: Members welcomed the fact that in its ruling of 6 October 2015, the CJEU declared invalid the Commission Adequacy Decision 2000/520/EC on the US Safe Harbour. They stressed that this ruling had confirmed the long-standing position of Parliament regarding the lack of an adequate level of protection under this instrument, and called on the Commission to immediately take the necessary measures to ensure that all personal data transferred to the US were subject to an effective level of protection that was essentially equivalent to that guaranteed in the EU.

Recalling that the Commission addressed 13 recommendations to the US in its communications of 27 November 2013 on the functioning of the Safe Harbour, Members objected to the fact that Parliament had not received any formal communication from the Commission regarding the state of implementation of the 13 recommendations, despite the Commissions announcement that it would do so by summer 2014. They underlined that, following the CJEUs decision to invalidate Decision 2000/520/EC, it was now urgent that the Commission provide a thorough update on the negotiations thus far and the impact of the judgment on the further negotiations that were announced. The Commission should reflect immediately on alternatives to Safe Harbour and on the impact of the judgment on any other instruments for the transfer of personal data to the US. Parliament called for a report on the matter by the end of 2015.

In addition, it

With regard to the EU-US Terrorist Finance Tracking Programme (TFTP) Agreement, Parliament was disappointed that the Commission disregarded Parliaments clear call for the suspension of the TFTP agreement, given that no clear information was given to clarify whether SWIFT data would have been accessed outside TFTP by any other US government body. It intended to take this into account when considering giving consent to future international agreements.

Democratic oversight: the resolution called on all those national parliaments which had not yet done so to thoroughly evaluate and install meaningful oversight of intelligence activities and to ensure that such oversight committees/bodies had sufficient resources, technical expertise and legal means and access to all relevant documents in order to be able to effectively and independently oversee intelligence services and information exchanges with other foreign intelligence services. Parliament noted that the lack of a common definition of national security in the EU and its Member States allowed for arbitrariness and abuses of fundamental rights and the rule of law by executives and intelligence communities in the EU.

Rebuilding trust: the resolution stressed that a healthy EU-US relationship remained absolutely vital for both partners. Revelations about surveillance had undermined public support for the relationship, and Parliament underlined the need to rebuild trust and find a negotiated solution between the US and the EU as a whole, respecting fundamental rights.

Protection of the rule of law and the fundamental rights of EU citizens/enhanced protection for whistleblowers and journalists: Members considered that EU citizens fundamental rights remained in danger and that too little had been done to ensure their full protection in case of electronic mass surveillance. It regretted that the Commission had not responded to Parliaments request to conduct an examination as to a comprehensive European whistleblower protection programme, and called on the Commission to present a communication on this subject, by the end of 2016 at the latest.

European strategy for greater IT independence: Members were disappointed by the lack of action by the Commission to follow up the detailed recommendations made in the resolution for increasing IT security and online privacy in the EU. They wanted to see the development of a European strategy for greater IT independence and online privacy within the framework of new initiatives such as the Digital Single Market.

Parliament welcomed the steps taken so far to strengthen Parliaments IT security, and called for the systematic replacement of proprietary software by auditable and verifiable open-source software in all the EU institutions, for the introduction of a mandatory open-source selection criterion in all future ICT procurement procedures, and for efficient availability of encryption tools.