US NSA surveillance programme, surveillance bodies in various Member States and impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs

2013/2188(INI) - 12/03/2014 - Text adopted by Parliament, single reading

The European Parliament adopted by 544 votes to 78 with 60 abstentions, a resolution 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.

Parliament noted that in comparison to actions taken both by EU institutions and by certain EU Member States, the European Parliament had taken very seriously its obligation to shed light on the revelations on the indiscriminate practices of mass surveillance of EU citizens and instructed its Committee on Civil Liberties, Justice and Home Affairs to conduct an in-depth inquiry into the matter.

Main findings: Members considered that recent revelations in the press by whistleblowers and journalists, together with the expert evidence given during this inquiry, admissions by authorities, and the insufficient response to these allegations, have resulted in **compelling evidence of the existence of far-reaching, complex and highly technologically advanced systems** designed by US and some Member States' intelligence services to collect, store and analyse communication data, including content data, location data and metadata of all citizens around the world, on an unprecedented scale and in an indiscriminate and non-suspicion-based manner.

Parliament specifically pointed to:

- US NSA intelligence programmes allowing for the mass surveillance of EU citizens through direct access to the central servers of leading US internet companies (PRISM programme), the analysis of content and metadata (Xkeyscore programme), the circumvention of online encryption (BULLRUN);

- systems of the UK intelligence agency GCHQ such as the upstream surveillance activity (Tempora programme), etc.

Parliament emphasised that trust had been profoundly shaken between the two transatlantic partners. In order to rebuild trust, **an immediate and comprehensive response plan** comprising a series of actions which were subject to public scrutiny was needed.

Noting that several governments claim that these mass surveillance programmes were necessary to combat terrorism, Parliament stated that the fight against terrorism could never be a justification for untargeted, secret, or even illegal mass surveillance programmes. It strongly rejected the notion that all issues related to mass surveillance programmes were purely a matter of national security and therefore the sole competence of Member States. Discussion and action at EU level were not only legitimate, but also a matter of EU autonomy.

Recommendations: the US authorities and the EU Member States were called upon **to prohibit blanket mass surveillance activities.** Parliament intended to request strong political undertakings from the new Commission to implement the proposals and recommendations of this Inquiry.

Members States were called upon to:

- comprehensively evaluate, and revise where necessary, their national legislation and practices governing the activities of the intelligence services so as to ensure that they are subject to parliamentary and judicial oversight and public scrutiny;

- immediately fulfil their positive obligation under the European Convention on Human Rights to protect their citizens from surveillance contrary to its requirements, including when the aim thereof is to safeguard national security, undertaken by third states or by their own intelligence services, and

- ensure that the rule of law is not weakened as a result of extraterritorial application of a third country's law.

The United Kingdom, France, Germany, Sweden, the Netherlands and Poland were specifically asked to ensure that their current or future legislative frameworks and oversight mechanisms governing the activities of intelligence agencies were in line with the standards of the European Convention on Human Rights and European Union data protection legislation and to clarify the allegations of mass surveillance activities. Member States were also asked to shed light on US intelligence personnel and equipment on EU territory **without oversight on surveillance operations.**

The Commission was called upon to:

- carry out, before July 2014, an assessment of the applicability of Regulation (EC) No 2271/96 to cases of conflict of laws on transfers of personal data;

- present measures providing for the immediate suspension of Commission Decision 520/2000, which declared the adequacy of the Safe Harbour privacy principles. In this respect, the US authorities are urged to put forward a proposal for a new framework for transfers of personal data from the EU to the US which meets Union law data protection requirements and provides for the required adequate level of protection;

- present, by December 2014, a comprehensive assessment of the US privacy framework covering commercial, law enforcement and intelligence activities, and concrete recommendations based on the absence of a general data protection law in the US;

- engage with the US administration in order to establish a legal framework providing for a high level of protection of individuals with regard to the protection of their personal data when transferred to the US and ensure the equivalence of EU and US privacy frameworks;

- conduct, before the end of 2014, an in-depth assessment of the **existing Mutual Legal Assistance Agreement;**

- immediately resume the negotiations with the US on the 'Umbrella Agreement', which should put rights for EU citizens on an equal footing with rights for US citizens and not initiating any new sectorial agreements or arrangements for the transfer of personal data with the US as long as the 'Umbrella Agreement' has not entered into force;

- react to concerns that three of the major computerised reservation systems used by airlines worldwide are based in the US and that PNR data are saved in cloud systems operating on US soil under US law, which lacks data protection adequacy;

- present, by December 2014, a proposal for an EU security clearance procedure for all EU office holders;

- present draft legislation to ban the use of backdoors by law enforcement agencies;

- present, by January 2015 at the latest, an **Action Plan to develop greater EU independence in the IT sector,** including a more coherent approach to boosting European IT technological capabilities (including IT systems, equipment, services, cloud computing, etc);

- put forward by December 2014, legislative proposals to encourage software and hardware manufacturers to introduce more security and privacy by design and by default features in their products, including by introducing disincentives for the undue and disproportionate collection of mass personal data and legal liability on the part of manufacturers for unpatched known vulnerabilities, faulty or insecure products or the installation of secret backdoors enabling unauthorised access to and processing of data;

- through funding in the **field of research and development**, support the development of European innovative and technological capability in IT tools, companies and providers (hardware, software, services and network), including for purposes of cybersecurity and encryption and cryptographic capabilities;

- put forward by December 2014, legislative proposals to encourage software and hardware manufacturers to introduce more security and privacy by design and by default features in their products, including by introducing disincentives for the undue and disproportionate collection of mass personal data and legal liability on the part of manufacturers for unpatched known vulnerabilities, faulty or insecure products or the installation of secret backdoors enabling unauthorised access to and processing of data.

Threat to block approval of the Transatlantic Trade and Investment Partnership Agreement (TTIP): the resolution stressed that that the consent of the European Parliament to the final TTIP agreement could be endangered as long as the blanket mass surveillance activities and the interception of communications in EU institutions and diplomatic representations were not completely abandoned and an adequate solution found for the data privacy rights of EU citizens. Parliament might only consent to the final TTIP agreement provided the agreement fully respected, inter alia, the fundamental rights recognised by the EU Charter, and provided the protection of the privacy of individuals in relation to the processing and dissemination of personal data remain governed by Article XIV of the GATS. Parliament stresses that EU data protection legislation could not be deemed an ‘arbitrary or unjustifiable discrimination’ in the application of Article XIV of the GATS.

Parliament called for the setting up of a High-Level Group to propose, in a transparent manner and in collaboration with parliaments, recommendations and further steps to be taken for:

- enhanced democratic oversight, including parliamentary oversight, of intelligence services

- increased oversight collaboration in the EU, in particular as regards its cross-border dimension;

- the possibility of **minimum European standards or guidelines** for the (ex ante and ex post) **oversight of intelligence services** on the basis of existing best practices and recommendations by international bodies;

- prepare a report for and to assist in the preparation of a conference to be held by Parliament with national oversight bodies, whether parliamentary or independent, by the beginning of 2015.

Parliament decides to launch '**A European Digital Habeas Corpus** - protecting fundamental rights in a digital age' with the following 8 actions, the implementation of which it will oversee:

- the adoption of the Data Protection Package in 2014;

- the conclusion of the EU-US Umbrella Agreement guaranteeing the fundamental right of citizens to privacy and data protection and ensuring proper redress mechanisms for EU citizens;

- the **suspension of Safe Harbour** (voluntary standards on data protection for non-EU businesses that send personal data of EU citizens to the US) until a full review has been conducted and current loopholes were remedied;

- the **suspension of the TFTP** agreement until: (i) the Umbrella Agreement negotiations have been concluded; (ii) a thorough investigation has been concluded on the basis of an EU analysis and all concerns raised by Parliament in its resolution of 23 October 2013 have been properly addressed;

- an examination from the Commission as to whether a future legislative proposal establishing an effective and comprehensive European whistleblower protection programme. Member States should thoroughly examine the possibility of granting whistleblowers international protection from prosecution;

- the development of a European strategy for greater IT independence.

Lastly, the competent services of the Secretariat of the European Parliament were asked to carry out, by June 2015 at the latest, a thorough review and assessment of **Parliament's IT security dependability**, focused on: budgetary means, staff resources, technical capabilities, internal organisation and all relevant elements, in order to achieve a high level of security for Parliament's IT systems.

Parliament instructed its Committee on Civil Liberties, Justice and Home Affairs to address Parliament in plenary on the matter a year after the adoption of this resolution, assessing the extent to which the recommendations adopted by Parliament had been followed and to analyse any instances where such recommendations had not been followed.