Human rights and technology: impact of intrusion and surveillance systems on human rights in third countries

2014/2232(INI) - 08/09/2015 - Text adopted by Parliament, single reading

The European Parliament adopted by 371 vote to 293, with 43 abstentions, a resolution concerning ‘Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries’.

Parliament recalled that technological developments and access to the open internet are playing an increasingly important role in enabling and ensuring the fulfilment and full respect for human rights and freedom of expression.

Information and communication technologies (ICTs) can be used as a tool to be able to intercept communications and data as the US National Security Agency (NSA) has done. The surveillance of communications interferes with the rights to privacy and expression, if conducted outside an adequate legal framework. Parliament stated that the active complicity of certain EU Member States in the NSA’s mass surveillance of citizens and spying on political leaders has caused serious damage to the credibility of the EU’s human rights policy and has undermined global trust in the benefits of ICTs.

Members called for further coherence between the EU’s external actions and its internal policies related to ICTs. The impact of technologies on the improvement of human rights should be mainstreamed in all EU policies and programmes, if applicable, to advance the protection of human rights and the promotion of democracy, the rule of law and good governance, and peaceful conflict resolution. They called on the EU to increase its support for actors who work on strengthening security and privacy protection standards in ICTs at all levels and called for a human rights and technology fund to be established under the European Instrument for Democracy and Human Rights.

Encryption software: Parliament urged the EU itself, and in particular the EEAS, to use encryption in its communications with human rights defenders, to avoid putting defenders at risk and to protect its own communications with outsiders from surveillance. It drew attention to the importance of developing ICTs in conflict areas to promote peacebuilding activities with a view to providing secure communication between parties involved in peaceful resolution of conflicts. Furthermore, it called on the Commission and the Council to further support, train and empower human rights defenders, civil society activists and independent journalists using ICTs in their activities in a safe manner.

Whistleblowers: Parliament drew attention to the plight of whistleblowers and their supporters, including journalists, following their revelations of abusive surveillance practices in third countries. It considered that such individuals should be considered human rights defenders and that, as such, they deserve the EU’ s protection, as required under the EU Guidelines on Human Rights Defenders. It reiterated its call on the Commission and the Member States to examine thoroughly the possibility of **granting whistleblowers international protection** from prosecution. Parliament called for measures to ensure that the privacy of activists, journalists and citizens is protected everywhere in the world and that they are able to network via the internet.

Fight against terrorism and protection of privacy: Parliament deplored the fact that security measures, including counterterrorism measures, are increasingly used as pretexts for violations of the right to privacy and for clamping down on the legitimate activities of human rights defenders, journalists and political

activists. According to Parliament, **national security can never be a justification for untargeted, secret or mass surveillance programmes**. It recognised that the internet has become a public space as well as a marketplace, for which the free flow of information and access to ICTs are indispensable. It called for the inclusion of clauses in all agreements with third countries that refer explicitly to the need to promote, guarantee and respect digital freedoms.

Democratic scrutiny: Parliament considered that mass surveillance that is not justified by a heightened risk of terrorist attacks and threats to be in violation of the principles of necessity and proportionality, and, therefore, a violation of human rights. It urged the Member States to promote **full democratic scrutiny of the operations of intelligence services in third countries**.

Members urged the EU to ensure greater transparency in the relationship between mobile phone carriers or ISPs and governments, and to call for it in its relations with third countries, by demanding that carriers and ISPs publish yearly detailed transparency reports.

It stressed the need to implement and monitor EU regulations and sanctions relating to ICTs more effectively, including the use of catch-all mechanisms, so as to ensure that all parties, including the Member States, comply with legislation and that a level playing field is preserved. In general, Parliament stressed the fact that respect for fundamental rights is an essential element in successful counter-terrorism policies, including the use of digital surveillance technologies.

Dual-use regime: Parliament urged the Commission to put forward a proposal for smart and effective policies to limit and regulate the commercial export of services regarding the implementation and use of so-called dual-use technologies, **addressing potentially harmful exports of ICT products and services to third countries**. It called on the Commission to include effective safeguards to prevent any harm of these export controls to research, including scientific and IT security research.

Members reaffirmed that EU standards, particularly the EU Charter of Fundamental Rights, should prevail in assessments of incidents involving dual-use technologies used in ways that may restrict human rights. They deplored the active co-operation of certain European companies, as well as of international companies trading in dual-use technologies with potential detrimental effects on human rights while operating in the EU, with regimes whose actions violate human rights. Parliament urged the Commission **publicly to exclude companies engaging in such activities from EU procurement procedures**, from research and development funding and from any other financial support.

Internet neutrality: it also urged the Commission and Council actively to defend the open internet, multi-stakeholder decision-making procedures, net neutrality, digital freedoms and data protection safeguards in third countries through internet governance. It called explicitly for the promotion of tools enabling the anonymous and/or pseudonymous use of the internet, and challenges the one-sided view that such tools serve only to allow criminal activities. Members recalled that mesh-based, ad hoc wireless technologies offer great potential in providing backup networks in areas where the internet is unavailable or blocked, and can help the advancement of human rights.

Encryption for all: Members called for **each individual to be entitled to encryption**, and for the conditions needed to allow encryption to be created. Controls should be a matter for the end user, who will need the skills required to carry out such controls properly. They also called for the introduction of 'end to end' encryption standards as a matter of course for all communication services, so as to make it more difficult for governments, intelligence agencies and surveillance bodies to read content. They emphasised the special responsibility of government intelligence services to build trust, and called for an **end to mass surveillance**.

Lastly, Parliament condemned the weakening and undermining of encryption protocols and products, particularly by intelligence services seeking to intercept encrypted communications.