Security and fundamental freedoms on the Internet

Increasingly, companies, governments, police and even criminals are seeking the greatest possible access to our private data. The internet provides a previously unimaginable level of access to information about our private lives, which unfortunately, can be abused by companies, intelligence services or even identity thieves. The report highlights action against cybercriminals whilst also guaranteeing fundamental rights to privacy for internet users.

The report adopted with 481 votes in favour, 25 against and 21 abstentions is the first recommendation from MEPs concerning the fight against cybercrime and preserving the rights of internet users. Clearly the internet can be used as an excellent tool for accessing information and allowing connections between individuals and communities all over the world. However, it also has its dangers as it can expose users to surveillance, or even serve as a tool for criminals or terrorists. The main advantage and disadvantage of the internet is that it transcends almost all borders.

Criminalising grooming

Parliament urges Member States to update legislation to protect children using the Internet, in particular in order to criminalise grooming (online solicitation of children for sexual purposes), as defined in the Council of Europe Convention of 25 October 2007 on the Protection of Children against Sexual Exploitation and Sexual Abuse.

MEPs are also concerned with the idea that "e-illiteracy will be the new illiteracy of the 21st Century." The report argues that in this age, having access to the internet is "equivalent to ensuring that all citizens have access to schooling", and that this access should not be denied by governments or private companies.

Fundamental freedoms of internet users

There are a number of fundamental rights which are affected by the internet, including "respect for private life...data protection...freedom of speech and association, freedom of press, political expression and participation, non-discrimination and education." The report calls on Member States to protect these rights by making use of existing national, regional, and international law, and to exchange best practices amongst themselves.

The report recognises that given "the global and open nature of the Internet", international standards for data protection, security and freedom of speech are required. MEPs call on Member States and the Commission to draw up a series of regulations to protect the privacy of internet users.

Crime, identity theft and terrorism
The nature of the internet also means that it is open to abuse. It has "been used as a platform for violent messages…as well as for websites which can specifically incite hate-based criminal acts." Cybercrime, in general has also increased, and internet users are at risk of identity theft, if they transmit their personal details across the internet without a minimum level of protection. Therefore, the House calls on the Council and Commission to develop a "comprehensive strategy to combat cybercrime…identity theft and fraud."

Finally, the report raises the question of consent of internet users, when giving personal information to governments or private companies, and the imbalance of negotiating power between users and institutions. In relation to this, MEPs stress the importance of internet users being able to retain the right to permanently delete any of their personal details saved on "internet websites or on any third party data storage medium."

Contact:

Baptiste CHATAIN
BXL: (32-2) 28 40992
STR: (33-3) 881 73603
PORT: (32) 498.983.590
EMAIL: libe-press@europarl.europa.eu

Richard FREEDMAN
E-mail: press-EN@europarl.europa.eu
BXL: (32-2) 28 41448
STR: (33-3) 881 73785
PORT: (+32) 498 98 32 39