Parliamentary Assembly
Assemblée parlementaire
http://assembly.coe.int
1949.2019
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

**Resolution 2256 (2019)**[1]

# Internet governance and human rights

Parliamentary Assembly

1. The internet is a common asset, the uses of which influence many aspects of daily life and also affect the effective enjoyment of human rights and fundamental freedoms. The internet has become so important that the future of our societies now also depends on the future of the internet. It is vital that the growth of the internet provide our societies with more information and knowledge, innovation and sustainable development, social justice and collective well-being, freedom and democracy. To achieve this goal, there is a compelling need to ensure more effective protection of human rights on the internet.

2. The numerous and well-thought-out texts adopted by the Committee of Ministers of the Council of Europe in this domain clearly show the crucial importance of these issues. The Parliamentary Assembly recalls, among others, the 2011 Declaration on Internet governance principles and the following recommendations: CM/Rec(2012)3 on the protection of human rights with regard to search engines; CM/Rec(2012)4 on the protection of human rights with regard to social networking services; CM/Rec(2013)1 on gender equality and media; CM/Rec(2014)6 on a Guide to human rights for Internet users; CM/Rec(2015)6 on the free, transboundary flow of information on the Internet; CM/Rec(2016)1 on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality; CM/Rec(2016)5 on Internet freedom; CM/Rec(2018)2 on the roles and responsibilities of internet intermediaries; and CM/Rec(2018)7 on Guidelines to respect, protect and fulfil the rights of the child in the digital environment.

3. The Assembly recognises universal access to the internet as a key internet governance principle and considers that the right to internet access, with no discrimination, is an essential component of any sound policy designed to promote inclusion and support social cohesion, as well as an essential factor of sustainable democratic and socio-economic development.

4. The Assembly highlights the importance of guaranteeing the right to an open internet, and of building an ecosystem which safeguards net neutrality. It notes that the economic players that control the operating systems and their application stores can impose unjustified restrictions on users' freedom of access to content and services available online, and that the risk of such restrictions increases with the transition towards ever smarter devices.

5. The Assembly underlines the need to guarantee the effective protection of the right to freedom of expression and freedom of information, online and offline, and the obligation incumbent on Council of Europe member States to ensure that this right, which is a pillar of any democratic society, is not threatened either by public authorities or private-sector or non-governmental operators. At the same time, more must be done to counteract the dangers brought about by abuses of the right to freedom of expression and information on the internet, such as incitement to discrimination, hatred and violence, aimed at women or ethnic, religious, sexual or other minorities in particular; child sexual abuse content; online bullying; the manipulation of information and propaganda; and incitement to terrorism.

6. This requirement is also connected with the necessity to guarantee that the internet becomes a secure environment in which users are protected from arbitrary action, threats, attacks on their physical and mental integrity and violations of their rights. Security must be reinforced with regard to the following: databases

1. *Assembly debate* on 23 January 2019 (6th Sitting) (see Doc. 14789, report of the Committee on Culture, Science, Education and Media, rapporteur: Mr Andres Herkel). *Text adopted by the Assembly* on 23 January 2019 (6th Sitting).
See also Recommendation 2144 (2019).

managed by public or private institutions; internet communications and transactions; vulnerable users and victims of racist or hate speech, of online bullying or of any other infringement of their dignity; the strategic infrastructures and key services that rely on the internet to operate; and our democratic societies, which are threatened by cyberterrorism and cyberwarfare.

7. Equally, the protection of privacy and personal data in cyberspace must be reinforced, to prevent the technologies that are now so much part of our daily lives from becoming a means of manipulating opinions and insidious checks on our private lives. In this respect, the Assembly underlines once more the threat to human rights posed by the large-scale systems set up by intelligence services for the mass collection, preservation and analysis of communications data, and it condemns unreservedly the deviations and abuses of power which, under the pretext of security, undermine the foundations of democracy and the rule of law. In addition, the Assembly is concerned that the interest of private companies in having easy access to and use of the greatest possible quantities of personal data still outweighs the protection of internet users, despite significant advances in this area.

8. If these challenges are to be successfully addressed, we must work together more effectively. The Assembly therefore calls for critical reflection on internet governance and underlines the crucial importance of the issue, which must be a core aspect of public policy, both at national level and in regional and global multilateral relations. It is vital that governments, the private sector, civil society, the academic and technical internet community and the media continue to engage in an open and inclusive dialogue, with a view to developing and implementing a shared vision of a digital society that is based on democracy, the rule of law and fundamental rights and freedoms. Dialogue platforms such as the global United Nations Internet Governance Forum (IGF), the European Dialogue on Internet Governance (EuroDIG) and the South Eastern European Dialogue on Internet Governance (SEEDIG), as well as the various national initiatives, help to foster such a shared vision and a better understanding of the respective roles and responsibilities of the stakeholders, and they can serve as catalysts for co-operation in the digital realm. In this respect, the Assembly also welcomes the decision taken by the United Nations Secretary-General on 12 July 2018 to establish the High-level Panel on Digital Cooperation, tasked with mapping trends in digital technologies, identifying gaps and opportunities, and outlining proposals for strengthening international co-operation.

9. The Assembly therefore recommends that the member States of the Council of Europe focus their internet governance work more effectively on the protection of human rights, fully implementing the recommendations of the Committee of Ministers in this domain and, in this context:

9.1. implement public investment policies which are coherent with the objective of universal access to the internet; these policies should be intended, in particular, to remedy the geographical imbalances (for example between urban and rural or remote areas), offset the digital divide between generations and eradicate gender inequalities, as well as other inequalities resulting from socio-economic and cultural gaps, or from disabilities;

9.2. be active in international forums to uphold net neutrality and safeguard this principle within the framework of national legislation, which should, *inter alia*:

9.2.1. clearly establish a principle of freedom of choice in content and applications, regardless of the device;

9.2.2. provide users with the right to delete pre-installed applications and easily access applications offered by alternative application stores, with the obligation of the economic players concerned to offer appropriate technical solutions to this end;

9.2.3. impose transparency on the indexing and ranking criteria employed by application stores and, in this respect, provide for the gathering of relevant information from device manufacturers;

9.2.4. provide for the recording of and following up of reports from end-users, and for developing comparison tools regarding the practices of the economic players concerned;

9.3. consider holistic policies for combating computer crime and abuse of the right to freedom of expression and information on the internet; such policies should draw not only on up-to-date criminal legislation but also on strengthened means of prevention, including the setting-up of police forces specialised in detecting and identifying online criminals and equipped with appropriate technical resources; awareness raising and improved education for users; enhanced co-operation with internet operators and greater accountability on their part;

9.4. ensure, at the same time, that any national decisions or actions involving restrictions on the right to freedom of expression and information comply with Article 10 of the European Convention on Human Rights (ETS No. 5) and prevent user protection and security requirements from becoming pretexts for silencing dissenting views and undermining media freedom;

9.5. recognise and implement effectively the "security by design" principle and, in this respect:

9.5.1. ensure that security is a fundamental design feature in the conception of the overall internet architecture and computer infrastructure of essential services, in order to reinforce resilience with regard to various forms of criminal or terrorist assaults and to reduce the risk and potential consequences of breakdowns;

9.5.2. provide for risk management and incident reporting obligations for operators of essential services and digital service providers;

9.5.3. promote stronger European and international co-operation aimed at achieving a high level of security of network and information systems;

9.5.4. advocate the development of harmonised international security standards concerning "the internet of things", including the establishment of a certification mechanism;

9.5.5. provide for the responsibility of private businesses (but also, where appropriate, of public authorities) for damages resulting from insufficient security of the connected objects they produce and commercialise, and introduce compulsory insurance schemes (entirely financed by the business sector) to mutualise risks.

10. The Assembly underlines that children need special protection online and that they need to be educated about how to steer clear of danger and to benefit as much as possible from the internet. The member States of the Council of Europe, together with all relevant stakeholders, must make full use of Committee of Ministers Recommendation CM/Rec(2018)7.

11. The Assembly considers that the Council of Europe Convention on Cybercrime (ETS No. 185, "Budapest Convention") should be better used to enhance interstate collaboration aimed at strengthening cybersecurity. The Assembly therefore calls on member States to:

11.1. ratify the Budapest Convention, if they have not yet done so, and ensure its full implementation, taking due account of the guidance notes on attacks on critical information infrastructure, distributed denial-of-service attacks, terrorism and other issues;

11.2. support the completion of the negotiation on the second additional protocol to the Budapest Convention on enhanced international co-operation and access to evidence of criminal activities in the cloud;

11.3. strengthen synergies between the Budapest Convention, the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201, "Lanzarote Convention") and the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence (CETS No. 210, "Istanbul Convention") to address cyberviolence, following the recommendations in the "Mapping study on cyberviolence" adopted by the Cybercrime Convention Committee (T-CY) on 9 July 2018;

11.4. support, and make best use of, the capacity-building programmes implemented by the Cybercrime Programme Office of the Council of Europe (C-PROC).

12. The Assembly encourages the member States of the Council of Europe to engage with the High-level Panel on Digital Cooperation established by the Secretary-General of the United Nations and contribute to its work. The Assembly recommends that the member States of the Council of Europe work together to improve, at both domestic and international levels, decision-making processes concerning the internet, advocating internet governance that is multi-stakeholder and decentralised, transparent and responsible, collaborative and participatory. In this respect, they should:

12.1. actively participate, including with their parliamentarians, in the IGF, the EuroDIG and other regional and national internet governance dialogue platforms;

12.2. promote the open nature of the decision-making process, so as to ensure the balanced participation of all interested parties, in varying ways depending on their specific role in relation to the issues being addressed, and aim, as far as possible, at consensual solutions, while avoiding stalemates;

12.3. enable the various groups of players themselves to administer the processes for appointing their representatives, but require that the procedures established for that purpose be open, democratic and transparent;

12.4. encourage an approach involving the re-composition of interests within various groups of stakeholders, for example through associations or federations that have to meet internal democracy criteria; concerning users' representation, encourage a balanced representation of gender, age and ethnicity;

12.5. develop, at the national level, multi-stakeholder mechanisms which should serve as a link between local discussions and the work of regional and global bodies; ensure fluent co-ordination and dialogue across those different levels and foster both a bottom-up approach (from the local to the multilateral level) and a top-down approach (from the multilateral to the local level);

12.6. avoid concentrating powers exclusively in the hands of public authorities and preserve the role of organisations tasked with technical aspects and aspects of internet management, as well as the role of the private sector;

12.7. seek to identify the decision-making centres that are most appropriate in terms of effectiveness, in the light of their knowledge of the problems to be dealt with and their ability to adapt solutions to the specific features of the communities responsible for ensuring their implementation, having also regard to the horizontal distribution of decision-making powers among players of different kinds;

12.8. require that all those participating in internet governance ensure the transparency of their actions, as this is an essential precondition of responsible governance. To this end:

12.8.1. it must be possible to identify each stakeholder's responsibility with regard to the final decision and its implementation;

12.8.2. at the multilateral level, the community of States should lay down clearer procedures, in consultation with other stakeholders;

12.8.3. the meaning of decisions taken should be comprehensible for those affected by them and these decisions should be made public and therefore be documented, categorised and published in such a way as to be easily available to everyone;

12.9. keep a proactive attitude to uphold the participatory and collaborative aspects of the decision-making process, and in this respect provide the partners concerned with the means of being meaningfully involved in decision making and move beyond the circle of professionals in this field, so that experts in other fields can contribute to the development of the internet.