SENATO DELLA REPUBBLICA

XVIII LEGISLATURA

Doc. XII-*bis*
n. 90

ASSEMBLEA PARLAMENTARE DEL CONSIGLIO D'EUROPA

Risoluzione n. 2256 (2019)

Internet e la *governance* dei diritti umani

Trasmessa il 31 gennaio 2019

PARLIAMENTARY ASSEMBLY OF THE COUNCIL OF EUROPE

RESOLUTION 2256 (2019) [1]

Provisional version

Internet governance and human rights

PARLIAMENTARY ASSEMBLY,

1. The internet is a common good, the uses of which influence many aspects of daily life and also affect the effective enjoyment of human rights and fundamental freedoms. The internet is 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 provides our societies with more information and knowledge, innovation and sustainable development, social justice and collective well-being, freedom and democracy. To achieve that 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 who control the operating systems and their app 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.

---

(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).

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 is not threatened by either 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, especially focusing on women or against ethnic, religious, sexual or other minorities; child sexual abuse content; online bullying; the manipulation of information and propaganda; as well as incitement to terrorism.

6. This requirement is also connected with the necessity to guarantee that the internet is 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: of the databases managed by public or private institutions; of internet communications and transactions; of vulnerable users, victims of racist and hate speech, of online bullying or of infringements of their dignity; of the strategic infrastructures and key services that rely on the internet to operate; of our democratic societies threatened by cyberterrorism and cyberwarfare.

7. Equally, the protection of privacy and personal data in the cyberspace must be reinforced, to avoid the technologies that are now so much part of our daily lives becoming a means of manipulating opinions and of 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 the intelligence services for the mass collection, preservation and analysis of communications data, and it condemns unreservedly the deviations and abuses of power which, under pretexts of security, undermine the foundations of democracy and the rule of law. In addition, the Assembly is concerned that the interest of private companies to have easy access to and use of the greatest amount 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 Pan-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 a 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 internet governance 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 fora 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 services, regardless of the device;

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

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

9.2.4. provide for recording and following up reports from end-users, and for developing comparison tools regarding the practices of the economic actors 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, and 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 for the main internet architecture and computer infrastructure of essential services, in order to reinforce resilience vis-à-vis various forms of criminal or terroristic 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 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 (to be 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 get maximum benefit from the internet. The member States of the Council of Europe, together with all relevant stakeholders, must make full benefit of Committee of Ministers Recommendation CM/Rec(2018)7 on Guidelines to respect, protect and fulfil the rights of the child in the digital environment.

11. The Assembly considers that the Council of Europe Convention on Cyber-

crime (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 critical information infrastructure attacks, distributed denial of service attacks, terrorism and other issues;

11.2. support the completion of the negotiation of 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 level, the 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, in the EuroDIG and in other regional and national internet governance dialogue platforms;

12.2. promote the open nature of the decision-making process, so as to ensure a 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 the procedures established for that purpose to 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 also ethnicity;

12.5. develop, at the national level, multi-stakeholder mechanisms which should serve as a link between local discussions and regional and global instances; 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 horizontal distribution of decision-making powers among players of different kinds;

12.8. require that all those participating in internet governance ensure 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.

ASSEMBLÉE PARLEMENTAIRE DU CONSEIL DE L'EUROPE

RÉSOLUTION 2256 (2019) [1]

Version provisoire

La gouvernance de l'internet et les droits de l'homme

ASSEMBLÉE PARLEMENTAIRE,

1. L'internet est un bien commun, dont les utilisations influencent de nombreux aspects de la vie au quotidien et touchent aussi la jouissance effective des droits de l'homme et des libertés fondamentales. L'importance de l'internet est telle que le futur de nos sociétés dépend désormais aussi du futur de l'internet. Il est essentiel que l'évolution de l'internet conduise nos sociétés vers plus d'information et de connaissance, d'innovation et de développement durable, de justice sociale et de bien-être collectif, de liberté et de démocratie. Pour atteindre cet objectif, il est impératif d'assurer une protection plus effective des droits de l'homme sur l'internet.

2. Les nombreux textes mûrement réfléchis adoptés en la matière par le Comité des Ministres du Conseil de l'Europe témoignent très clairement de l'importance cruciale que revêtent ces questions. L'Assemblée parlementaire rappelle, entre autres, la Déclaration sur des principes de la gouvernance de l'internet de 2011 et les recommandations suivantes: CM/Rec(2012)3 sur la protection des droits de l'homme dans le contexte des moteurs de recherche; CM/Rec(2012)4 sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux; CM/Rec(2013)1 sur l'égalité entre les femmes et les hommes et les médias; CM/Rec(2014)6 sur un Guide des droits de l'homme pour les utilisateurs d'internet; CM/Rec(2015)6 sur la libre circulation transfrontière des informations sur internet; CM/Rec(2016)1 sur la protection et la promotion du droit à la liberté d'expression et du droit à la vie privée en lien avec la neutralité du réseau; CM/Rec(2016)5 sur la liberté d'internet; CM/Rec(2018)2 sur les rôles et les responsabilités des intermédiaires d'internet; et CM/Rec(2018)7 sur les Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique.

3. L'Assemblée reconnaît l'accès universel à internet en tant que principe clé de la gouvernance de l'internet et considère que le droit d'accès sans discrimination à internet est une composante essentielle de toute politique solide visant à promouvoir l'inclusion et à soutenir la cohésion sociale, ainsi qu'un facteur essentiel du développement durable démocratique et socio-économique.

4. L'Assemblée souligne l'importance de garantir le droit à un internet ouvert et de bâtir un écosystème qui sauvegarde la neutralité du Net. Elle note que les acteurs

---

(1) *Discussion par l'Assemblée* le 23 janvier 2019 (6e séance) (voir Doc. 14789, rapport de la commission de la culture, de la science, de l'éducation et des médias, rapporteur: M. Andres Herkel). *Texte adopté par l'Assemblée* le 23 janvier 2019 (6e séance).
Voir également la Recommandation 2144 (2019).

économiques qui contrôlent les systèmes d'exploitation et leurs magasins d'applications peuvent imposer des limitations non justifiées à la liberté d'accès des utilisateurs aux contenus et aux services disponibles en ligne, et que le risque de telles limitations s'accroît avec l évolution vers des terminaux toujours plus intelligents.

5. L'Assemblée rappelle la nécessité d'assurer une protection effective du droit à la liberté d'expression et d'information, en ligne et hors ligne, ainsi que l'obligation pour les États membres du Conseil de l'Europe de veiller à ce que ce droit, pilier de toute société démocratique, ne soit menacé ni par les pouvoirs publics ni par les opérateurs du secteur privé ou non gouvernemental. En même temps, il faut faire plus pour contrer les dangers que les abus du droit à la liberté d'expression et d'information sur l'internet engendrent, tels que l'incitation à la discrimination, à la haine et à la violence, ciblant en particulier les femmes ou contre les minorités ethniques, religieuses, sexuelles ou autres, le contenu concernant l'abus sexuel d'enfants, le cyberharcèlement, la manipulation de l'information et la propagande, ainsi que l'incitation au terrorisme.

6. Cette exigence se lie aussi à la nécessité de garantir que l'internet soit un environnement sécurisé, où les usagers sont à l'abri de l'arbitraire, des menaces, des attentes à l'intégrité physique et psychique et des violations de leurs droits. Il faut renforcer la sécurité des bases de données que les institutions publiques ou privées gèrent; des échanges et transactions sur le réseau; des usagers vulnérables, victimes de propos racistes et haineux, de cyberharcèlement ou de toute autre atteinte à leur dignité; des infrastructures stratégiques et des services essentiels qui s'appuient sur l'internet pour leur fonctionnement; de nos sociétés démocratiques menacées par le cyberterrorisme et la guerre cybernétique.

7. Il faut également renforcer la protection de la vie privée et des données personnelles dans le cyberespace, pour éviter que les technologies qui font désormais partie de notre quotidien deviennent des outils de manipulation des opinions et de contrôle sournois de notre vie privée. À cet égard, l'Assemblée souligne à nouveau la menace que représentent pour les droits de l'homme les systèmes d'envergure mis en place par les services de renseignement en vue de collecter, de conserver et d'analyser à une grande échelle les données des communications, et condamne sans réserves les dérives et les abus de pouvoir qui, sous des prétextes sécuritaires, sapent les fondements de la démocratie et de l'État de droit. Par ailleurs, l'Assemblée est préoccupée par le fait que l'intérêt des entreprises privées à avoir un accès aisé au plus grand nombre de données personnelles et de les utiliser librement l'emporte encore sur la protection des utilisateurs d'internet, malgré les avancées significatives dans ce domaine.

8. Pour faire face à ces défis avec succès, il faut oeuvrer ensemble plus efficacement. Ainsi, l'Assemblée prône une réflexion critique sur la gouvernance de l'internet et souligne l'importance cruciale de cette question, qui doit être au coeur des politiques publiques tant au niveau national que dans le cadre des relations multilatérales régionales et globales. Il est essentiel que les gouvernements, le secteur privé, la société civile, la communauté universitaire et technique des internautes et les médias continuent d'entretenir un dialogue ouvert et inclusif afin de définir et de concrétiser une vision commune d'une société numérique fondée sur la démocratie, l'État de droit et les libertés et droits fondamentaux. Les plates-formes de dialogue telles que le Forum des Nations Unies sur la gouvernance de l'internet (FGI), de portée mondiale, le Dialogue paneuropéen sur la gouvernance de l'internet (EuroDIG) et le Dialogue européen du Sud-Est sur la gouvernance de l'internet (SEEDIG), ainsi que les diverses initiatives nationales, contribuent à favoriser une telle vision commune et une meilleure compréhension des responsabilités et rôles respectifs des parties prenantes, et elles peuvent jouer le rôle de catalyseur de coopération dans le monde numérique. À cet égard, l'Assemblée salue également la décision prise le 12 juillet 2018 par le Secrétaire général des Nations Unies de créer un Groupe de haut niveau sur la coopération numérique, chargé de présenter les tendances de l'évolution des technologies numériques, de recenser les ca-

rences et les perspectives qu'elles recèlent et de proposer des moyens de renforcer la coopération internationale.

9. Dès lors, l'Assemblée recommande aux États membres du Conseil de l'Europe de mieux centrer la gouvernance de l'internet sur la protection des droits de l'homme, en donnant pleinement application aux recommandations du Comité des Ministres dans ce domaine et, dans ce contexte:

9.1. de mettre en oeuvre des politiques nationales d'investissement public cohérentes avec l'objectif d'un accès universel à internet; ces politiques devraient viser en particulier à corriger les déséquilibres géographiques (par exemple entre les zones urbaines et les zones rurales ou isolées), à aplanir le fossé numérique entre les générations et à éradiquer les inégalités de genre, ainsi que d'autres inégalités dues aux différences socio-économiques et culturelles ou à des handicaps;

9.2. d'être actifs dans les instances internationales pour garantir la neutralité du Net et sauvegarder ce principe dans le cadre de la législation nationale, qui devrait, entre autres:

9.2.1. établir clairement le principe de liberté de choix des contenus et applications quel que soit le terminal;

9.2.2. prévoir le droit des utilisateurs de supprimer des applications préinstallées et d'accéder aisément aux applications proposées par des magasins d'applications alternatifs, avec l'obligation pour les acteurs économiques concernés d'offrir des solutions techniques adéquates à cette fin;

9.2.3. imposer la transparence des critères de référencement et de classement employés par les magasins d'applications et, à cet égard, prévoir la collecte de l'information pertinente auprès des fabricants de terminaux;

9.2.4. prévoir l'enregistrement et le suivi des signalements des utilisateurs finals, ainsi que le développement d'outils de comparaison entre les pratiques des acteurs économiques concernés;

9.3. de réfléchir à des politiques globales de lutte contre la criminalité informatique et contre les abus du droit à la liberté d'expression et d'information sur internet; ces politiques devraient s'appuyer non seulement sur une législation pénale à jour, mais aussi sur le renforcement des moyens de prévention, y compris l'établissement de forces de police spécialisées dans le dépistage et l'identification des criminels informatiques et dotées de moyens techniques adéquats, la sensibilisation et une meilleure éducation des utilisateurs, ainsi qu'une collaboration accrue avec les opérateurs de l'internet et leur responsabilisation;

9.4. d'assurer, en même temps, que toute décision ou action nationale entraînant une restriction du droit à la liberté d'expression et d'information soit conforme à l'article 10 de la Convention européenne des droits de l'homme (STE no 5) et éviter que la protection des utilisateurs et les exigences sécuritaires ne deviennent un prétexte pour museler les opinions dissidentes et pour porter atteinte à la liberté des médias;

9.5. de reconnaître et mettre en oeuvre efficacement le principe de la «sécurité dès la conception» et, à cet égard:

9.5.1. assurer que la sécurité soit un trait fondamental dans la conception de l'architecture principale de l'internet et des infrastructures informatiques des services essentiels, afin de renforcer la résilience vis-à-vis des diverses formes d'attaques terroristes ou criminelles et de réduire le risque et les conséquences potentielles des pannes;

9.5.2. prévoir des obligations de gestion des risques et de signalement des incidents pour les opérateurs de services essentiels et les fournisseurs de services numériques;

9.5.3. prôner une coopération européenne et internationale accrue visant à assurer un niveau élevé commun de sécu-

rité des réseaux et des systèmes d'information;

9.5.4. promouvoir le développement des normes de sécurité internationales harmonisées concernant «l'internet des objets», y compris la mise en place d'un mécanisme de certification;

9.5.5. prévoir la responsabilité des entreprises privées (mais aussi, le cas échéant, des autorités publiques) en cas de dommages dus à une sécurité insuffisante des objets connectés qu'elles produisent et commercialisent, et introduire des régimes d'assurance obligatoire (entièrement financés par le secteur privé) afin de mutualiser les risques.

10. L'Assemblée souligne que les enfants nécessitent une protection spécifique en ligne et doivent être éduqués sur la manière d'éviter les dangers et de bénéficier au maximum d'internet. Les États membres du Conseil de l'Europe, avec les autres parties prenantes, doivent tirer entièrement parti de la Recommandation CM/Rec(2018)7 du Comité des Ministres sur les Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique.

11. L'Assemblée considère que la Convention du Conseil de l'Europe sur la cybercriminalité (STE no 185, «Convention de Budapest») devrait être mieux utilisée pour améliorer la collaboration interétatique visant à renforcer la cybersécurité. Par conséquent, l'Assemblée appelle les États membres:

11.1. à ratifier la Convention de Budapest, s'ils ne l'ont pas encore fait, et à garantir sa pleine mise en oeuvre, en tenant dûment compte des notes d'orientation sur les attaques visant les infrastructures d'information critiques, sur les attaques par déni de service distribué, sur le terrorisme et sur d'autres questions;

11.2. à encourager l'achèvement des négociations du deuxième protocole additionnel à la Convention de Budapest sur une coopération internationale renforcée et l'accès aux preuves d'activités criminelles stockées dans le nuage («cloud»);

11.3. à renforcer les synergies entre la Convention de Budapest, la Convention du Conseil de l Europe sur la protection des enfants contre l exploitation et les abus sexuels (STCE no 201, «Convention de Lanzarote» et la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique (STCE no 210, «Convention d'Istanbul») pour remédier à la cyberviolence, en suivant les recommandations figurant dans l'étude cartographique sur la cyberviolence adoptée par le Comité de la Convention Cybercriminalité (T-CY) le 9 juillet 2018;

11.4. à soutenir, et à utiliser au mieux, les programmes de renforcement des capacités menés par le Bureau de programme du Conseil de l Europe sur la cybercriminalité (C-PROC).

12. L'Assemblée encourage les États membres du Conseil de l'Europe à s'engager avec le Groupe de haut niveau sur la coopération numérique créé par le Secrétaire général des Nations Unies et de contribuer à ses travaux. L'Assemblée recommande aux États membres du Conseil de l'Europe d'oeuvrer ensemble pour améliorer, tant au niveau interne qu'au niveau international, les processus de prise de décision sur les questions concernant l'internet, en prônant une gouvernance de l'internet qui soit multipartite et décentralisée, transparente et responsable, collaborative et participative. À cet égard, ils devraient:

12.1. participer activement, y compris avec leurs parlementaires, au FGI, à l'EuroDIG et à d'autres plateformes de dialogue régionales et nationales sur la gouvernance de l'internet;

12.2. promouvoir le caractère ouvert du processus de prise de décision, afin d'assurer une participation équilibrée des parties qui y ont intérêt, selon des modalités variables en fonction du rôle qui est le leur par rapport aux questions traitées,

et rechercher, dans la mesure du possible, des solutions consensuelles, tout en évitant les situations de blocage;

12.3. permettre que les différents groupes d'acteurs puissent administrer eux-mêmes les processus de désignation de leurs représentants, mais exiger que les procédures établies à cette fin soient ouvertes, démocratiques et transparentes;

12.4. encourager une dynamique de recomposition des intérêts au sein des divers groupes de parties prenantes, par exemple par le biais de structures associatives/fédératives devant respecter les critères d'une démocratie interne; concernant la représentation des usagers, encourager une représentation équilibrée selon les sexes, l'âge ainsi que l'origine ethnique;

12.5. développer, au niveau national, des mécanismes multipartites qui devraient servir de lien entre les discussions menées à l'échelle locale et les instances intervenant à l'échelle régionale et mondiale; assurer une bonne coordination et une communication fluide entre ces différents niveaux et favoriser une dynamique qui soit à la fois ascendante (du niveau local au niveau multilatéral) et descendante (du niveau multilatéral au niveau local);

12.6. éviter de concentrer les pouvoirs décisionnels dans les mains des autorités publiques et préserver le rôle des organisations chargées des aspects techniques et des aspects de gestion de l'internet, ainsi que le rôle du secteur privé;

12.7. viser à identifier les centres de décision les plus appropriés en termes d'efficacité, en raison de la connaissance des problèmes à traiter et de la capacité d'adapter les solutions aux spécificités des communautés qui doivent assurer leur mise en oeuvre, en ayant égard également à une répartition horizontale des compétences décisionnelles entre acteurs de nature différente;

12.8. exiger que tous ceux qui participent à la gouvernance de l'internet assurent la transparence de leur action, celle-ci étant une condition sine qua non d'une gouvernance responsable. À cette fin:

12.8.1. il faut pouvoir identifier quelle responsabilité chacune des parties prenantes assume par rapport à la décision finale et à sa mise en œuvre;

12.8.2. au niveau multilatéral, la communauté des États devrait définir des procédures décisionnelles plus claires, en consultation avec les autres parties prenantes;

12.8.3. le sens des décisions prises doit être compréhensible pour leurs destinataires et ces décisions doivent être publiques, donc documentées, classifiées et publiées de manière à être aisément accessibles à tous;

12.9. maintenir une attitude proactive pour soutenir les caractères participatif et collaboratif du processus de décision; à cet égard, donner aux partenaires concernées les moyens de participer utilement à la prise de décision et inclure dans ces processus des experts d'autres domaines, au-delà du cercle des professionnels du métier, afin qu'ils puissent également contribuer au développement de l'internet.

ASSEMBLEA PARLAMENTARE DEL CONSIGLIO D'EUROPA

RISOLUZIONE 2256 (2019)

Internet e la *governance* dei diritti umani

ASSEMBLEA PARLAMENTARE,

1. Internet è un bene comune, il cui uso influenza molti aspetti della vita quotidiana e si ripercuote sul pieno godimento dei diritti umani e delle libertà fondamentali. Internet è così importante che il futuro delle nostre società ormai dipende anche dal futuro di Internet. È essenziale che la crescita di Internet fornisca alle nostre società maggiore informazione e conoscenza, innovazione e sviluppo sostenibile, giustizia sociale e benessere collettivo, libertà e democrazia. Per conseguire tale obiettivo, è assolutamente necessario garantire una più efficace protezione dei diritti umani su Internet.

2. I numerosi testi, ben ponderati, adottati dal Comitato dei Ministri del Consiglio d'Europa in questo ambito mostrano chiaramente l'importanza vitale di tali questioni. L'Assemblea Parlamentare richiama, tra le altre, la Dichiarazione del 2011 sui principi della *governance* di Internet e le seguenti raccomandazioni: CM/Rec(2012)3 sulla protezione dei diritti umani relativamente ai motori di ricerca; CM/Rec(2012)4 sulla protezione dei diritti umani nell'ambito dei servizi di *social network*; CM/Rec(2013)1 sull'uguaglianza di genere e i media; CM/Rec(2014)6 relativa a una Guida ai diritti umani per gli utenti di Internet; CM/Rec(2015)6 sulla libera circolazione transfrontaliera delle informazioni su Internet; CM/Rec(2016)1 sulla protezione e la promozione del diritto alla libertà di espressione e del diritto alla vita privata in relazione alla neutralità della rete; CM/Rec(2016)5 sulla libertà di Internet; CM/Rec(2018)2 su ruoli e responsabilità degli intermediari di Internet; e CM/Rec(2018)7 sulle linee guida per il rispetto, la protezione e la realizzazione dei diritti dei minori nell'ambiente digitale.

3. L'Assemblea riconosce l'accesso universale a Internet come un principio fondamentale della governance di Internet e ritiene che il diritto all'accesso a Internet senza discriminazioni sia una componente essenziale di qualunque politica valida volta a promuovere l'inclusione e a sostenere la coesione sociale, oltre ad essere un fattore essenziale di sviluppo sostenibile democratico e socioeconomico.

4. L'Assemblea sottolinea l'importanza di garantire il diritto a un'Internet aperta e di costruire un ecosistema che salvaguardi la neutralità della Rete. Essa rileva che gli attori economici che controllano i sistemi operativi e i loro negozi di app possono imporre restrizioni ingiustificate alla libertà degli utenti di accedere ai contenuti e ai servizi disponibili on-line, e che il rischio di tali restrizioni aumenta man mano che si transita verso dispositivi sempre più intelligenti.

5. L'Assemblea sottolinea la necessità di garantire un'efficace protezione del diritto alla libertà di espressione e alla libertà di

informazione, in rete e fuori dalla rete, e l'obbligo per gli Stati membri del Consiglio d'Europa di garantire che tale diritto non sia minacciato né dalle autorità pubbliche né da operatori del settore privato o non governativo. Allo stesso tempo, occorre fare di più per contrastare i pericoli provocati dagli abusi del diritto alla libertà di espressione e di informazione su Internet, quali: l'istigazione alla discriminazione, all'odio e alla violenza, soprattutto contro le donne o contro minoranze etniche, religiose, sessuali o di altro genere; contenuti pedopornografici; bullismo in rete; la manipolazione di informazioni e la propaganda nonché l'istigazione al terrorismo.

6. Tale esigenza è legata anche alla necessità di garantire che Internet sia un ambiente sicuro, nel quale gli utenti sono protetti da azioni arbitrarie, minacce, attacchi alla loro integrità fisica e mentale e violazioni dei loro diritti. Occorre rinforzare la sicurezza: dei database gestiti da istituzioni pubbliche o private; delle comunicazioni e transazioni su Internet; degli utenti vulnerabili, vittime di discorsi razzisti e di odio, del bullismo in rete o di violazioni della loro dignità; delle infrastrutture strategiche e dei servizi essenziali il cui funzionamento sia basato su Internet; delle nostre società democratiche minacciate dal terrorismo cibernetico e dalla guerra cibernetica.

7. Analogamente, occorre aumentare la protezione della vita privata e dei dati personali nello spazio cibernetico, per evitare che le tecnologie che ormai occupano gran parte della nostra quotidianità diventino uno strumento per manipolare le opinioni e controllare in modo insidioso le nostre vite private. In relazione a ciò, l'Assemblea sottolinea ancora una volta la minaccia per i diritti umani rappresentata dai sistemi su vasta scala creati dai servizi di intelligence per la raccolta, la conservazione e l'analisi di una grande quantità di dati delle comunicazioni e condanna senza riserve le deviazioni e gli abusi di potere che, con il pretesto della sicurezza, minacciano le fondamenta della democrazia e dello stato di diritto. In aggiunta a ciò l'Assemblea è preoccupata per il fatto che l'interesse delle società private ad accedere facilmente e utilizzare un'enorme quantità di dati personali continui a prevalere rispetto alla protezione degli utenti di Internet, nonostante i significativi passi avanti registrati in questo ambito.

8. Se vogliamo affrontare con successo queste sfide, dobbiamo lavorare insieme in modo più efficace. Per questo l'Assemblea chiede che si aprì una riflessione critica sulla governance di Internet e sottolinea l'importanza essenziale di tale questione, che deve rappresentare un aspetto centrale delle politiche pubbliche, sia a livello nazionale che nelle relazioni multilaterali regionali e globali. È fondamentale che i governi, il settore privato, la società civile, il mondo accademico e la comunità tecnica di Internet e i media continuino a mantenere un dialogo aperto e inclusivo, al fine di sviluppare e attuare una visione condivisa di una società digitale basata sulla democrazia, lo stato di diritto e i diritti e le libertà fondamentali. Piattaforme di dialogo quali il Forum globale delle Nazioni Unite sulla governance di Internet (IGF), il Dialogo europeo sulla governance di Internet (EuroDIG) e il Dialogo paneuropeo sud-orientale sulla governance di Internet (SEEDIG), oltre alle varie iniziative nazionali, aiutano a promuovere tale visione condivisa e una migliore comprensione dei ruoli e delle responsabilità dei diversi attori e possono fungere da catalizzatori della cooperazione nel settore digitale. Al riguardo, l'Assemblea accoglie con favore anche la decisione assunta dal Segretario Generale delle Nazioni Unite il 12 luglio 2018 di costituire un Gruppo di Alto Livello sulla cooperazione digitale, incaricato di mappare le tendenze del settore delle tecnologie digitali, individuare lacune e opportunità ed elaborare proposte per rafforzare la cooperazione internazionale.

9. L'Assemblea pertanto raccomanda che gli Stati membri del Consiglio d'Europa concentrino la *governance* di Internet in modo più efficace sulla tutela dei diritti umani, dando piena attuazione alle rac-

comandazioni del Comitato dei Ministri in questo ambito e, in tale contesto:

9.1. attuino politiche di investimento pubbliche che siano coerenti con l'obiettivo di un accesso universale a Internet; tali politiche dovrebbero essere volte, in particolare, a risolvere gli squilibri geografici (ad esempio tra zone urbane e zone rurali o remote), colmare il divario digitale tra le generazioni ed eliminare le diseguaglianze di genere, oltre ad altre diseguaglianze derivanti da divari socioeconomici e culturali o da disabilità;

9.2. siano attivi nelle sedi internazionali per salvaguardare la neutralità della Rete e tutelare questo principio nel quadro delle legislazioni nazionali, che dovrebbero, tra le altre cose:

9.2.1. introdurre esplicitamente il principio della libertà di scelta di contenuti e servizi, a prescindere dal dispositivo;

9.2.2. prevedere il diritto degli utenti di cancellare applicazioni preinstallate e accedere facilmente ad applicazioni offerte da negozi di app alternativi, con l'obbligo per gli attori economici interessati di offrire a tal fine soluzioni tecniche adeguate;

9.2.3. Imporre la trasparenza dei criteri di indicizzazione e posizionamento utilizzati dai negozi di app e, al riguardo, prevedere la raccolta di informazioni pertinenti presso i produttori di dispositivi;

9.2.4. prevedere la registrazione e l'elaborazione delle segnalazioni provenienti dagli utenti finali e la messa a punto di strumenti di confronto tra le pratiche degli attori economici interessati;

9.3. valutino la possibilità di elaborare politiche olistiche per contrastare la criminalità informatica e l'abuso del diritto alla libertà di espressione di informazione su Internet; tali politiche dovrebbero basarsi non solo su normative penali aggiornate, ma anche su strumenti di prevenzione rafforzati, che includano la creazione di forze di polizia specializzate nell'individuare e identificare criminali in rete e dotate di risorse tecniche adeguate, attività di sensibilizzazione e una migliore educazione per gli utenti e un rafforzamento della cooperazione con gli operatori di Internet e una maggiore trasparenza da parte di questi ultimi;

9.4. garantiscano, allo stesso tempo, che qualunque decisione o azione nazionale che preveda restrizioni del diritto alla libertà di espressione e di informazione sia in linea con l'Articolo 10 della Convenzione Europea dei Diritti dell'Uomo (STE n° 5) ed eviti che la tutela degli utenti e i motivi di sicurezza diventino una scusa per silenziare voci dissenzienti e minare la libertà dei media;

9.5. riconoscano e attuino in maniera efficace il principio della« « sicurezza dalla progettazione » e, al riguardo:

9.5.1. garantiscano che la sicurezza sia un elemento fondamentale nella progettazione dell'architettura principale di Internet e delle infrastrutture informatiche dei servizi essenziali, al fine di aumentare la resilienza nei confronti delle varie forme di attacchi criminali o terroristici e ridurre il rischio e le potenziali conseguenze di guasti;

9.5.2. prevedano obblighi di gestione dei rischi e denuncia di incidenti per gli operatori dei servizi essenziali e i fornitori dei servizi digitali;

9.5.3. promuovano una maggiore cooperazione europea e internazionale al fine di conseguire un alto livello di sicurezza delle reti e dei sistemi di informazione;

9.5.4. sostengano lo sviluppo di standard di sicurezza internazionali armonizzati per ciò che concerne « l'Internet delle cose », inclusa la creazione di un meccanismo di certificazione;

9.5.5. prevedano la responsabilità delle aziende private (ma anche, se necessario, delle autorità pubbliche) per i danni derivanti da una insufficiente sicurezza degli oggetti connessi che esse producono e commercializzano, e introducano polizze

assicurative obbligatorie (interamente finanziate dal settore privato) per mutualizzare i rischi.

10. L'Assemblea sottolinea che i minori hanno bisogno di una protezione speciale on-line e che devono essere educati per imparare a stare lontani dai pericoli e ottenere il massimo beneficio da Internet. Gli Stati membri del Consiglio d'Europa, insieme a tutti gli attori coinvolti, devono trarre il massimo vantaggio dalla raccomandazione del Comitato dei Ministri CM/Rec(2018)7 sulle linee guida per rispettare, proteggere e realizzare i diritti dei minori nell'ambiente digitale.

11. L'Assemblea ritiene che occorrerebbe fare un uso migliore della Convenzione del Consiglio d'Europa sulla criminalità informatica (STE n° 185, « Convenzione di Budapest ») per rafforzare la collaborazione tra Stati e aumentare la sicurezza cibernetica. L'Assemblea pertanto invita gli Stati membri a:

11.1. ratificare la Convenzione di Budapest, qualora non lo abbiano ancora fatto, e garantire la sua piena attuazione, tenendo conto delle Note di Orientamento sugli attacchi alle infrastrutture informatiche critiche, gli attacchi di negazione di servizio distribuita, terrorismo e altre questioni;

11.2. appoggiare il completamento del negoziato del secondo protocollo aggiuntivo alla Convenzione di Budapest sul rafforzamento della cooperazione internazionale e l'accesso alle prove che riguardino attività criminali su *cloud*;

11.3. rafforzare le sinergie tra la Convenzione di Budapest, la Convenzione del Consiglio d Europa per la protezione dei bambini contro lo sfruttamento e gli abusi sessuali (STCE n° 201, « Convenzione di Lanzarote ») e la Convenzione di Istanbul sulla prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica (CETS n° 210, « Convenzione di Istanbul ») per contrastare la violenza cibernetica, seguendo le raccomandazioni formulate nello Studio di mappatura sulla violenza cibernetica adottato dal Comitato della Convenzione sulla criminalità informatica (T-CY) il 9 luglio 2018;

11.4. sostenere e fare l'uso migliore dei programmi di rafforzamento delle capacità attuati dall'Ufficio del programma contro la criminalità cibernetica del Consiglio d'Europa (C-PROC).

12. L'Assemblea esorta gli Stati membri del Consiglio d'Europa a interagire con il Gruppo di Alto Livello sulla Cooperazione Digitale istituito dal Segretario Generale delle Nazioni Unite e contribuire al suo lavoro. L'Assemblea raccomanda che gli Stati membri del Consiglio d'Europa lavorino insieme per migliorare, sia a livello nazionale che a livello internazionale, i processi decisionali riguardanti Internet, sostenendo una governance di Internet che sia multilaterale e decentralizzata, trasparente e responsabile, collaborativa e partecipativa. Al riguardo, essi dovrebbero:

12.1. partecipare attivamente, anche con i loro parlamentari, all'IGF, all'EuroDIG e ad altre piattaforme di dialogo sulla governance di Internet regionali e nazionali;

12.2. promuovere la natura aperta del processo decisionale, in modo da garantire una partecipazione equilibrata di tutte le parti interessate, con modalità variabili a seconda del loro ruolo specifico in relazione alle questioni affrontate e mirare, per quanto possibile, a soluzioni consensuali, evitando situazioni di stallo;

12.3. consentire ai vari gruppi di attori di gestire i processi per la nomina di propri rappresentanti, esigendo però che le procedure a tal fine siano aperte, democratiche e trasparenti;

12.4. incoraggiare un approccio che preveda la ricomposizione degli interessi all'interno dei vari gruppi di attori, ad esempio attraverso associazioni o federazioni tenute a rispettare criteri di democrazia interna; in merito alla rappresentanza di utenti, incoraggiare una rappre-

sentanza equilibrata per genere, età e anche etnia;

12.5. sviluppare, a livello nazionale, meccanismi multilaterali che servano da raccordo tra dibattiti locali e istanze regionali e globali; garantire un coordinamento e un dialogo fluidi tra i vari livelli e promuovere sia un approccio ascendente (dal livello locale a quello multilaterale) che un approccio discendente (dal livello multilaterale a quello locale);

12.6. evitare la concentrazione di poteri esclusivamente nelle mani delle autorità pubbliche e preservare il ruolo delle organizzazioni incaricate di occuparsi degli aspetti tecnici e degli aspetti della gestione di Internet, così come il ruolo del settore privato;

12.7. cercare di individuare i centri decisionali più adeguati in termini di efficacia, alla luce della conoscenza che essi hanno dei problemi da affrontare e della loro capacità di adattare le soluzioni alle caratteristiche specifiche delle comunità responsabili di garantirne l'attuazione, tenendo conto anche della distribuzione orizzontale dei poteri decisionali tra attori di tipo diverso;

12.8. chiedere che tutti coloro che partecipano alla governance di Internet garantiscano la trasparenza delle loro azioni, essendo questa una precondizione essenziale per una gouvernance responsabile. A tal fine:

12.8.1. deve essere possibile individuare la responsabilità di ciascun attore in relazione alla decisione finale e alla sua attuazione;

12.8.2. a livello multilaterale, la comunità degli Stati dovrebbe elaborare procedure più chiare, in consultazione con altri attori;

12.8.3. il significato delle decisioni assunte dovrebbe essere comprensibile per coloro che sono toccati da tali decisioni e queste ultime dovrebbero essere rese pubbliche e quindi essere documentate, classificate e pubblicate in modo da poter essere facilmente accessibili a tutti;

12.9. mantenere un atteggiamento proattivo per salvaguardare gli aspetti partecipativi e collaborativi del processo decisionale, e al riguardo fornire ai partner interessati gli strumenti per poter partecipare in modo significativo al processo decisionale e andare oltre la cerchia dei professionisti del settore, affinché esperti di altri settori possono contribuire allo sviluppo di Internet.

180122054440