Parliamentary Assembly
Assemblée parlementaire
http://assembly.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
1949.2019

Doc. 14789
04 January 2019

Internet governance and human rights

Report[1]
Committee on Culture, Science, Education and Media
Rapporteur: Mr Andres HERKEL, Estonia, Group of the European People's Party

Summary

The internet is a common good and its governance must be a core aspect of public policy, both at national level and in regional and global multilateral relations.

It is vital that there is an open and inclusive dialogue among governments, the private sector, civil society, the academic and technical internet community and the media, 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.

Member States are invited to fully implement the recommendations of the Committee of Ministers in this domain. The report calls for public investment policies that are coherent with the objective of universal access to the internet, the commitment of member States to uphold Net neutrality, holistic policies for combating computer crime and abuse of the right to freedom of expression and information on the internet, and an effective implementation of the "security by design" principle.

Member States should make better use of the Convention on Cybercrime to enhance interstate collaboration and they should engage with the United Nations High-level Panel on Digital Cooperation and contribute to its work, advocating internet governance that is multi-stakeholder, decentralised, transparent, responsible, collaborative and participatory.

[1] Reference to committee: Doc. 13280, Reference 4000 of 30 September 2013.

Contents **Page**

A. Draft resolution[2]

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.

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

[2] Draft resolution adopted unanimously by the committee on 6 December 2018

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 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 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.

B. Draft recommendation[3]

1. The Parliamentary Assembly, recalling its Resolution … (2019) on internet governance and human rights, highly values the work of the Council of Europe in the domain of the information society and underlines the key role of the Organisation in advocating stronger recognition of the human rights of internet users and their effective protection on the web, as well as its contribution to enhanced decision-making on internet governance issues. The numerous and well-thought-out texts adopted by the Committee of Ministers in this domain clearly show the crucial importance of these issues.

2. Internet governance should continue to be given high priority, as decisions in this domain have a direct impact on the life of all Europeans and on the future of our societies, including the stability of their democratic foundations and of their socio-economic development.

3. In this respect, the Assembly considers that additional efforts should be made to promote enhanced internet governance and help Council of Europe member States to act together to take up the challenges they have to face in this domain.

4. Internet governance requires clearer procedures, based on transparency and accountability. These procedures should be laid down by the community of States in consultation with other stakeholders in accordance with a multi-stakeholder approach. At European level, the Council of Europe and the European Union should act together to this end.

5. A first step in this direction could be to strengthen the political impact of the Pan-European dialogue on Internet governance (EuroDIG), so that it can play a more significant role in setting the agenda and in seeking to structure the debate on internet governance across the European continent. The Council of Europe should take a more proactive stance towards those European countries which do not have a national initiative, by encouraging such initiatives and taking care of their inclusiveness. An active commitment and support of the Council of Europe is of high importance to guarantee a minimum level of participation from all regions of Europe in the EuroDIG dialogue.

6. The Assembly is concerned about the insufficient security of network and information systems. In this respect, it commends the approach which is promoted within the European Union by Directive (EU) 2016/1148 on security of network and information systems, concerning measures for a high common level of security of network and information systems across the Union, namely improved cybersecurity capabilities at national level; increased European Union-level co-operation; and risk management and incident reporting obligations for operators of essential services and digital service providers. The Assembly considers that this approach should be encouraged in all Council of Europe member States and, possibly, the expertise acquired by the European Union and its members could be shared within the wider European framework and beyond.

7. Therefore, the Assembly recommends that the Committee of Ministers:

   7.1. entrust the Steering Committee on Media and Information Society (CDMSI) to monitor the implementation of the recommendations adopted by the Committee of Ministers in the field of internet governance, making good use of multi-stakeholder dialogue and results of internet governance fora such as the United Nations Internet Governance Forum (IGF), the Pan-European dialogue on Internet governance (EuroDIG), as well as other regional and national initiatives;

   7.2. launch a study on how to strengthen the existing forms of co-operation in the field of prevention of cyberattacks and on the expediency of creating a specific mechanism of monitoring, crisis management and post-crisis analysis by sharing resources that already exist in various countries, for example based on the model of the EUR-OPA Major Hazards Agreement.

[3] Draft recommendation adopted unanimously by the committee on 6 December 2018.

C. Explanatory memorandum by Mr Andres Herkel, rapporteur

1. Introduction: rational and scope of the report

1.1. Why internet governance matters

1. The internet is a "transformative phenomenon, with the capacity to touch nearly every aspect of life";[4] it is a kind of core superstructure for the functioning of all the others which are essential for our societies. Internet users are estimated to be more than 4.15 billion people, i.e. more than 54% of the world population.[5] According to Eurostat, in 2017, internet users amounted to 84% of the population of the European Union aged between 16 and 74.[6] We communicate between ourselves, access and consume content (including news and information which are crucial for informed citizens' choices and the functioning of our democracies), trade goods and services, manage our bank accounts, dialogue with our local and national administrations, have access to services (health, social care, justice, among others), pay our tax contributions and participate in political processes through the internet.

2. It is therefore self-evident that internet governance is a sensitive crucial global public policy issue. Sensitive, because of the inherent complexity of problems of a legal and technical nature that are posed, also resulting from the transnational nature of the internet communication flow which goes beyond nation States' sovereign borders. Crucial, also, because today the internet must be considered a common good, impacting on many aspects of our lives and touching upon our fundamental rights.

3. Our future is closely linked to the way the internet will develop. The report on *One Internet* by the Global Commission on Internet Governance (2016) captures the main risks and hopes in three possible scenarios. There are certainly many more which could result from less radical trends and from a combination of the key elements featuring each of these three scenarios; but I find this somewhat simplified vision quite useful for operational purposes.

4. The first – scary – scenario is a "dangerous and broken cyberspace", where, among others, unprecedented private data collection and government mass surveillance destroy users' privacy, sovereign-driven restrictions fragment the internet and violate human rights, malicious actions of cyber-criminals multiply undermining users security and the risk of cyberwarfare increases, including threats to the operation of civilian infrastructure such as the power grid or water systems.

5. The second scenario is one leading to "uneven and unequal gains", where some users capture a disproportionate share of "digital dividends" while others are permanently locked out. Governments do not preserve the internet's openness, do not enable competition and do not encourage the private sector to expand high-speed access. They choose to assert sovereign control through trade barriers, data localisation and censorship and by adopting other techniques that fragment the network in ways that limit the free flow of goods, services, capital and data.

6. The third, more optimistic, scenario is that of a healthy internet triggering "broad, unprecedented progress" and providing opportunities for social justice, human rights, access to information and knowledge, growth, development and innovation.

7. In this respect, our task as policy makers seems clear: to ensure that internet governance is able to deliver the best scenario, avoiding unwise, self-centred attitudes and behaviours which would divert the process towards alternative worrying developments.[7]

1.2. What "internet governance" means

8. The Tunis Agenda, adopted at the second phase of the World Summit on the Information Society in November 2005, provides a "working definition" of internet governance as the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures and programmes that shape the evolution and use of the internet.[8]

[4] See the introduction of the final report on One Internet by the Global Commission on Internet Governance (2016), published by the Centre for International Governance Innovation (CIGI) and Chatham House.

[5] See: Internet World Stats, internet usage statistics, at www.internetworldstats.com.

[6] http://ec.europa.eu/eurostat/web/products-datasets/-/tin00028.

[7] Concerns about the risks of a future internet, no longer free and open, are also being raised at the heart of the internet founders' community. See, for example, the statements by Sir Tim Berners-Lee at the Lisbon Web Summit (4-7 November 2019) or the analysis in moz://a Internet Health Report 2018.

9. This definition (that the Committee of Ministers of the Council of Europe takes up in its Recommendation CM/Rec(2007)16 on measures to promote the public service value of the Internet) is not necessarily perfect and it is not uncontested. However, I believe it offers a good starting point for our analysis:

– it points to the plurality of actors, with different (somewhat interconnected) roles, who are – and should remain – involved in internet governance, although in this respect I would certainly add to the list the international organisations (both at global and regional levels);

– it highlights the need to build the internet and regulate its use based on foundations which should be "shared", starting by agreeing on a core set of principles;

– in a less explicit way, it recognises that "internet governance is concerned not only with the internet's design and administration, but also with its evolution and use, so internet governance is inherently oriented towards the future and the impact on society".[9]

10. The Tunis Agenda definition seems to reflect the view of internet governance as a kind of monolithic system, thus masking an extremely complex reality, including the fact that governance arrangements may eventually vary in different domains.[10] To deal with this complexity, the report on One Internet by the Global Commission on Internet Governance has suggested that "[i]t can be helpful to think about the internet in layers. There are many possible taxonomies for these layers, but one simple framework … disaggregates components of the internet into four layers: infrastructure; logical; application; and content".[11] The same report also stresses that significant policy questions permeate all of these layers.

11. In this report, I will mainly refer to policy issues that are more closely linked with the "application layer" (including, for example, mobile apps, search engines, social media platforms and platforms for sharing user-generated content) and with the "content layer" (including text, audio, pictures, video and multimedia of all kinds). The policy issues in question could possibly be captured by the following sentence: There is a compelling need to ensure more effective protection of human rights on the internet. Though, I will use the term "internet governance", I wish to note here that the term "digital governance" is becoming more and more frequently used to encompass all governance aspects that go along with the digital transformation of our economic, social and political lives based on the spread of digital services and applications that use the internet and other digital technologies and infrastructure.

1.3. Key issues and focus of the report

12. From different texts of the Council of Europe[12] and of other stakeholders,[13] it appears very clearly that human rights, democracy and the rule of law are – and must remain – key goals of internet governance. Here, I will limit myself to quoting the Declaration on Internet governance principles, which was adopted by the Committee of Ministers of the Council of Europe on 21 September 2011. The first principle is on "Human rights, democracy and the rule of law":

> *"Internet governance arrangements must ensure the protection of all fundamental rights and freedoms and affirm their universality, indivisibility, interdependence and interrelation in accordance with international human rights law. They must also ensure full respect for democracy and the rule of law and should promote sustainable development. All public and private actors should recognise and uphold human rights and fundamental freedoms in their operations and activities, as well as in the design of new technologies, services and applications. They should be aware of developments leading to the enhancement of, as well as threats to, fundamental rights and freedoms, and fully participate in efforts aimed at recognising newly emerging rights."*

[8] www.itu.int/net/wsis/docs2/tunis/off/6rev1.html.

[9] See the introduction of the final report on One Internet, op. cit.

[10] See in this respect Mark Raymond and Laura DeNardis, Multistakeholderism: Anatomy of an Inchoate Global Institution, Paper Series No. 41, September 2016, published by the Centre for International Governance Innovation and Chatham House. The authors also stated that the formulation of this definition (though affirming the multi-stakeholder nature of internet governance) was arguably not a multi-stakeholder effort.

[11] A more articulated taxonomy is proposed by Mark Raymond and Laura DeNardis in their paper on "Multistakeholderism: Anatomy of an Inchoate Global Institution".

[12] I have included relevant texts of the Committee of Ministers in the document AS/Cult/Inf (2018) 08 rev.

[13] See, among others: the Charter of Human Rights and Principles for the Internet and the Ten Punchy Principles, delivered in 2011 by the Internet Rights & Principles Coalition (IRPC); both documents are included in a booklet published in different languages; the final NETmundial Multistakeholder Statement of 24 April 2014; the set of fourteen Principles for Internet Policy Making delivered in 2014 by the Organisation for Economic Co-operation and Development (OECD).

13. In the subsequent sections, I will first focus on a shortlist of fundamental rights which we must preserve together, taking account of specific threats that endanger them. In this analysis, I will build on the work of the Council of Europe intergovernmental sector and on our own very rich, previous work.

14. It is not enough to reaffirm that human rights must be at the core of internet governance; indeed this seems to be fairly consensual. Therefore, I will consider how we could enhance decision making on internet governance issues, and to what extent it is possible for the Council of Europe and for its member States to operate more effectively within the existing internet governance ecosystem to uphold these rights and secure their concrete implementation.

15. The compass of this report intercepts issues which have already been examined or are being discussed by our committee, as well as by the intergovernmental sector of the Council of Europe. Therefore, while seeking to provide a comprehensive overview and some updating, I do not intend to redo analyses that we have already performed and I will not discuss key questions which are covered by ongoing targeted committee work.

2. Human rights at stake

16. When we speak of the internet, the first right that comes to mind is the right to freedom of expression and information, which is inextricably linked to the internet today: it is essential to guarantee the freedom to express oneself and access content disseminated by others on the web. Other rights in this connection are freedom of thought, conscience and religion and freedom of assembly and association. However, essentially, the exercise of these freedoms in cyberspace is intertwined with that of freedom of expression and information.

17. In order for everyone to be able to fully enjoy these rights, there must first of all be a guarantee of access to the internet. It is also necessary to ensure that the internet remains an open ecosystem. In this connection, “Net neutrality” is based on two pillars: the obligation for internet access providers (IAPs) to treat all content transmitted on the web equally and the possibility for internet users to view and freely disseminate content on the web. At the same time, it is necessary to ensure users’ right to security and to respect for their privacy, especially from the point of view of the protection of personal data.

2.1. The right to internet access, with no discrimination

18. I would like to clarify, straightaway, that when I refer to a “right to internet access”, I do not mean an entitlement for everyone to have access to the internet free of charge, but rather a right to an affordable access to the free internet. In its Resolution 1987 (2014) on the right to Internet access, the Assembly holds that internet access as such should be recognised as a fundamental right. The report of the Committee on Culture, Science, Education and Media[14] stressed that actions and views by several governments, international actors – including the Council of Europe – and internet stakeholders pointed in this direction, and it referred to a wide recognition of the importance of the internet for freedom of expression[15] (but also of other rights), the promotion of the public service value of internet and case law from national and international courts. In this respect, the Committee of Ministers, in its Declaration on Internet governance principles, stated that “Internet-related policies should recognise the global nature of the Internet and the objective of universal access”.[16]

[14] Doc. 13434 (rapporteur: Ms Jaana Pelkonen, Finland, EPP/CD).

[15] The report quoted in particular: Nicola Lucchi, “Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression” (6 February 2011), *Cardozo Journal of International and Comparative Law* (JICL), Vol. 19, No. 3, 2011. Available at SSRN: https://ssrn.com/abstract=1756243.

[16] In the same line of thinking, among other examples, the United Nations Special Rapporteur on promotion and protection of the right to freedom of opinion and expression, Frank La Rue, in his report to the Human Rights Council of 16 May 2011, stated that: “The Internet, as a medium by which the right to freedom of expression can be exercised, can only serve its purpose if States assume their commitment to develop effective policies to attain universal access to the Internet” (document A/HRC/17/27, section 60). NETmundial 2014 states that internet governance should promote universal, equal opportunity, affordable and high quality internet access, so as to be an effective tool for enabling human development and social inclusion.

19. In some States, the legislation recognises (affordable) internet access as a right. For example, since 2000, internet access is a right under the Estonian legislation.[17] Since 2007 in Switzerland, the Telecommunications Act[18] has guaranteed the right to quality internet access at an affordable price to all inhabitants irrespective of where they live. Since 2009, in Finland, all individuals and businesses are considered to have the right to high-speed internet access in their place of residence.[19] More generally, at European Union level, Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) seeks to ensure the availability of a minimum set of good-quality electronic communications services accessible to all users at an affordable price.

20. It might be difficult for a number of countries, including in Europe, to formally proclaim internet access as a right per se, given the implication this would have in terms of infrastructure development (and related costs for the public budget) to ensure this right effectively. I believe however that not only should we ask that universal access to the internet be recognised as a key internet governance principle, but that we should encourage in Europe national public investment policies coherent with this objective, as its attainment seems to me an essential factor of sustainable democratic and socio-economic development.

21. The right to internet access certainly implies offsetting geographical imbalances (e.g. between urban and rural or remote areas); but it requires – and implies – much more. There is a clear digital divide between generations,[20] as well as socio-economic and cultural gaps. There are disabilities which require specific consideration and targeted action in order to ensure that certain categories of users could have proper access to internet facilities. There are also gender inequalities which impact significantly on internet access.[21] In this respect, the proportion of women using the internet is 12% lower than the proportion of men using it worldwide; and even in Europe the internet user gender gap between men and women is still close to 8%.[22] It is encouraging, however, that this gap has decreased since previous measurements and in some countries the penetration rate is equal.

22. In other terms, the right to internet access is an essential component of any sound policy designed to fight against discrimination, promote inclusion and support social cohesion. Here we are at the core of State responsibilities and this cannot just be handed over to the private sector.

23. There are good arguments also to convince those of us that are more focused on the economic dimension of (and budgetary constraints to) public policies. Just as an interesting example concerning gender discrimination, a 2015 McKinsey Global Institute report[23] holds that gender inequality is not only a pressing moral and social issue, but also a critical economic challenge and considers that, in a "full potential" scenario in which women and men play an identical role in labour markets, up to 28 trillion dollars could be added to global gross domestic product (GDP) by 2025. Of course, we cannot envisage closing gender gaps in work and society without closing the internet gap.[24]

24. The *One Internet* report suggests that governments need not only to encourage the continuing improvement of internet infrastructure, use competition as a tool to expand internet access facilities and invest to ensure availability when market forces prove insufficient, but they should also: develop public investment at locations such as schools and libraries to provide wider access to communities that would otherwise have

[17] Section 33 of the Estonian Public Information Act (*State Gazette*, 2000, 92, 597, passed on 15 November 2000) states that every person shall be afforded the opportunity to have free access to public information through the Internet in public libraries, pursuant to the procedure provided for in the Public Libraries Act.

[18] See: https://www.admin.ch/opc/en/classified-compilation/19970160/index.html.

[19] Following an amendment of section 60.c of the Communications Market Act (393/2003), which came into force on 1 July 2009.

[20] According to the ICT facts and Figures 2017, the proportion of young people aged 15 to 24 using the internet (71% worldwide; 95.7% in Europe) was significantly higher than the proportion of the total population using the internet (48% worldwide; 79.5% in Europe).

[21] On this issue, see among others, the analysis on Empowering women on the Internet, prepared in 2015 by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs.

[22] According to the *ICT Facts and Figures 2017*, the Internet penetration rate for men is 50.9% worldwide (82.9% in Europe) and for women is 44.9% (76.3% in Europe). The internet users gender gap is calculated as the difference between the internet user penetration rates for males and females relative to the internet user penetration rate for males, expressed as a percentage.

[23] How advancing women's equality can add $12 trillion to global growth (September 2015).

[24] See for example the following *Harvard Business Reviews*: Bhaskar Chakravorti, There's a Gender Gap in Internet Usage. Closing It Would Open Up Opportunities for Everyone (12 December 2017), and Julie Sweet, Access to Digital Technology Accelerates Global Gender Equality (17 May 2016).

limited opportunities due to factors such as income or geography; develop digital literacy; create incentives for the adoption of web standards intended to ensure that everyone, regardless of their physical capacities, can use the internet.

2.2. The right to an open internet: building an ecosystem which safeguards Net neutrality

25. The Declaration on Internet governance principles, when establishing the *Architectural principles*, asks that "[t]he open standards and the interoperability of the Internet as well as its end-to-end nature" be preserved and states that "[t]here should be no unreasonable barriers to entry for new users or legitimate uses of the Internet, or unnecessary burdens which could affect the potential for innovation in respect of technologies and services". In this respect, the phenomenon of innovative tools bought at their early stages by powerful internet platforms raises concerns about the real possibility for new competitors to emerge on a global scale through purely free-market mechanisms.[25]

26. Next, this declaration insists on the principle of *Open network*: "Users should have the greatest possible access to Internet-based content, applications and services of their choice, whether or not they are offered free of charge, using suitable devices of their choice." And then it continues: "Traffic management measures which have an impact on the enjoyment of fundamental rights and freedoms, in particular the right to freedom of expression and to impart and receive information regardless of frontiers, … must meet the requirements of international law on the protection of freedom of expression and access to information."

27. More recently, the Committee of Ministers, in its Recommendation CM/Rec(2015)6 on the free, transboundary flow of information on the internet (adopted on 1 April 2015), after recalling that "[t]he provisions on rights and freedoms set out in the European Convention on Human Rights … and Article 19 of the International Covenant on Civil and Political Rights apply equally online and offline", notes that "Article 10 of the [European Convention on Human Rights] applies not only to the content of information, but also to the means of dissemination or hosting, since any restriction imposed on the means of dissemination necessarily interferes with the right to receive and impart information". The Committee of Ministers then adds: "The unimpeded, transboundary flow of information on the Internet is critical for the full realisation of these rights and freedoms, safeguarding pluralism and diversity of information, the development of culture, education and innovation, and economic growth."

28. Here, I would also mention Committee of Ministers Recommendation 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 (adopted on 13 January 2016). This recommendation contains a set of guidelines on network neutrality in terms of equal treatment of internet traffic, pluralism and diversity of information, privacy, transparency and accountability; it calls on European States to safeguard the principle of network neutrality in the development of national legal frameworks in order to ensure the protection of the right to freedom of expression and to access to information, and the right to privacy.

29. Regulation (EU) 2015/2120[26] enshrines the principle of Net neutrality and guarantees an open internet access. It provides for the individual and enforceable right for end-users in the European Union to access and distribute internet content and services of their choice and for equal and non-discriminatory treatment of traffic in the provision of internet access services.[27] The Regulation also imposes obligations on internet access

[25] See, for example, here a list, updated in January 2018, with 66 Facebook acquisitions.

[26] Regulation (EU) 2015/2120 of the European Parliament and of the Council of the European Union of 25 November 2015 laying down measures concerning open internet access.

[27] Article 3.1 provides that "[e]nd-users shall have the right to access and distribute information and content, use and provide applications and services, and use terminal equipment of their choice, irrespective of the end-user's or provider's location or the location, origin or destination of the information, content, application or service, via their internet access service." Article 3.3 requires that "[p]roviders of internet access services shall treat all traffic equally, when providing internet access services, without discrimination, restriction or interference, and irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used". Additional information is available at the web page of the European Commission on the Open Internet.

Nonetheless, the rights of end-users (and the corresponding obligations of internet access providers) are not absolute: firstly, there are limits laid down by EU and domestic law with regard to the lawfulness of content, applications and services (Article 3.1, 2nd paragraph); secondly, the Regulation (Article 3.3, 2nd paragraph) authorises providers of internet access services to implement "reasonable traffic management measures". It continues that, in order to be deemed reasonable, measures "shall be transparent, non-discriminatory and proportionate, and shall not be based on commercial considerations but on objectively different technical quality of service requirements of specific categories of traffic". Furthermore, these measures "shall not monitor the specific content and shall not be maintained for longer than necessary".

providers to ensure transparency (Article 4), especially as regards the content of any contract that includes internet access services, and requires national regulatory authorities to ensure Net neutrality and respect for users' rights (Article 5).

30. However, the principle of Net neutrality has been challenged by the United States Federal Communications Commission (FCC) which repealed federal rules (with effect from 11 June 2018) intended to ensure Net neutrality. Thus, in the United States, cable and phone giants can now establish "fast lanes" for specific preferred sites and services (their own and/or those of their clients that are ready to pay more to get preferential treatment), everyone else being assigned slower lanes. They could also decide (in theory) to block access to some services, those of competitors for example.[28]

31. European users are protected by the EU legislation and the European Commissionaire, Andrus Ansip, publicly declared that the repeal of the US net neutrality rules will produce no effect in Europe. However, we are not "isolated" from what happens in other areas of the world – and especially in the United States – and I can hardly believe that there will be no impact whatsoever, including in terms of advantages or disadvantages for European businesses which operate at global level. Europe has a number of controversial files to deal with with the Trump Administration, which could appear more important; but internet governance should not be neglected and we should be active in all possible international fora to uphold Net neutrality.

32. In addition, Net neutrality is under threat, in Europe too, from both different forms of "State censorship" – which some regimes employ to silence their critics – and certain operator practices. I will briefly discuss issues concerning freedom of expression and freedom of information on the Net, including State censorship, in the following section.

33. As far as operator practices contrary to Net neutrality are concerned, I would like to mention here the report published in February 2018 by the French Regulatory Authority for Postal and Electronic Communications (ARCEP) entitled "Smartphones, tablets, voice assistants: devices, the weak link in achieving an open internet". This very instructive report points out very clearly that the internet access chain does not stop at access networks and that users' ability to access the desired content and services online can be (and indeed is) hampered by other intermediaries. In this connection, ARCEP points the finger at devices (smartphones, tablet, PCs, etc.), their operating systems and their app stores, which are controlled by a small number of economic players. It notes that "users' freedom of choice is being reduced by the restrictions this equipment imposes. Some of these restrictions may be warranted for reasons of design, security or innovation. Others artificially restrict internet access and the array of content and services available to users. The transition towards ever smarter devices – smart speakers at home, on-board computers in cars, connected products – raises concerns of ever increasing restrictions, within environments that are not always compatible with each other".[29]

34. To counter this risk, ARCEP identifies avenues for action (to be found on page 61 of its report), which should be brought to the attention of all our member States:

– clarifying what constitutes internet openness, by establishing a principle of freedom of choice in content and services, regardless of the device;

– "data-driven" regulation (gathering information from device manufacturers, gathering reports from end-users, promoting comparison tools, imposing transparency on the indexing and ranking criteria employed by app stores);

– increasing fluidity;

– lifting certain restrictions artificially imposed by key device market players and, in this connection, among other things, enabling users to delete pre-installed apps and easily access applications offered by alternative app stores, once they have been deemed reliable;

– establishing a rapid procedure for supporting businesses, especially small and medium-sized enterprises (SMEs) and start-ups, when they encounter questionable practices.

[28] The game in the United States is, however, not over yet: in addition to public reactions and legal procedures which consumer rights groups and some State attorney generals started against the FCC decision, the latter also raised opposition within the US Congress and in a number of States. For example, in the States of Washington Vermont, Oregon and California, new laws imposing equal treatment of data have come into force to replace the expired federal rules.

[29] ARCEP press release of 15 February 2018.

2.3. The right to freedom of expression and freedom of information

35. I have lost count of the number of times our committee and our Parliamentary Assembly have stressed the fundamental importance of the right to freedom of expression and information – enshrined in Article 10 of the European Convention on Human Rights and Article 19 of the United Nations Covenant on Civil and Political Rights – as a pillar of every democratic society. We have emphasised 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.

36. We have repeatedly stressed in our reports the role played by the internet and the social media in the new media context by putting an end to the concentration of the power to disseminate information, changing the communication paradigm, and radically modifying institutional communication and the relationship between the electorate and political parties, and between citizens, elected representatives and government departments.

37. We have also pointed out the new dangers brought about by abuses of the right to freedom of expression and information on the internet: incitement to discrimination, hatred and violence against ethnic, religious or other minorities; incitement to terrorism; child pornography; online bullying and violence against women; and the manipulation of information and propaganda for the purposes of political or other forms of destabilisation. This report will not revisit those issues, especially as they are regularly dealt with in more specific reports, including those prepared or currently being prepared by our committee.[30] We have carried out a full analysis but are still seeking effective solutions as it is hard to combat abuses without jeopardising the right to freedom of expression and information itself.

38. According to the Declaration on Internet governance principles, "[a]ny national decision or action amounting to a restriction of fundamental rights should comply with international obligations and in particular be based on law, be necessary in a democratic society and fully respect the principles of proportionality and the right of independent appeal, surrounded by appropriate legal and due process safeguards". While the declaration uses the conditional "should", this principle is clearly linked with Article 10 of the European Convention on Human Rights; thus, it is not negotiable. However, its proper implementation is far from being ensured.

39. Measures to close down websites may prove necessary to ensure the protection of users. However, if the actual aim is, for example, to prevent dissidence and undermine the activities of the democratic opposition, then this is a serious breach of freedom of expression in general and of freedom of the media in particular. Apart from serious and systemic breaches of the right to freedom of expression and information by regimes with little or no democracy, the extent of this right (i.e. its limits laid down by national legislation) may vary from one (democratic) country to another. This is not necessarily an anomaly as it is also a question of striking a balance between this right and other rights worthy of protection, and each national community expresses its own preferences in this regard. However, when it comes to the internet, these differences may become an obstacle to a sufficiently harmonised regulation of the legality (or otherwise) of content.

40. In addition, the progressive transformation of some search engines and social media into organised and active selectors of news and information for their users could trigger a serious impact on access to a variety of media and of opinions.[31]

41. Finally, I want to stress at this point the link between the right to freedom of expression and information and the possibility of enhancing cultural diversity and specific local characteristics without ending up with a kind of internet community isolationism. In this respect, according to the Declaration on Internet governance principles, "[p]reserving cultural and linguistic diversity and fostering the development of local content, regardless of language or script, should be key objectives of Internet-related policy and international co-operation, as well as in the development of new technologies".

[30] These are namely the reports on: Media freedom as a condition for democratic elections (Doc. 14669); Public service media in the context of disinformation and propaganda (Doc. 14780); Social media: social threads or threats to fundamental freedoms?; Towards an Internet Ombudsman institution; Media education in the new media environment; Threats to media freedom and journalists' security in Europe.

[31] This important question is dealt with in our committee's report on "Social media: social threads or threats to fundamental freedoms?".

2.4. Internet governance and security

42. Security is a fundamental right. We all aspire to live in a secure environment in which we are protected from arbitrary action, threats, attacks on our physical and mental integrity and violations of our rights. As the title of Article 5 of the European Convention on Human Rights reminds us, “liberty and security” go together. This also applies to the internet, as an integral part of our living environment. We speak of the “virtual” world, but it should be clearly understood that what happens on the web is part of our real life, and we need much more internet security. The speech of the French President Emmanuel Macron at the Paris Internet Governance Forum (12 to 14 November 2018)[32] was a cry of alarm that we should not ignore.

43. There are various aspects to this question, including:

- the security of the databases managed by public or private institutions which must be protected against malicious hacking aimed at stealing, manipulating, rendering inaccessible or destroying the data in question;
- the security of internet communications and transactions and combating computer fraud;
- the personal security of vulnerable users – children, young people, women and others – victims of racist and hate speech, of psychological violence, of infringements of their dignity and of online bullying;
- the security of the strategic infrastructures and key services that rely on the internet to operate, such as communication networks, energy networks (including the security of nuclear power stations), transport systems, the banking system and the stock exchange, and the health or justice services, the malfunctioning of which may have extremely serious or even dramatic consequences;
- more generally, the security of our democratic societies against all types of attack, including on our democratic institutions, linked to what is referred to as cyberterrorism and cyberwarfare.

44. This issue has, in its various aspects, been the subject of several documents produced by the Assembly (and our committee).[33] Guided both by the Assembly’s recommendations and by the proposals made by many experts, I would like to emphasise at this point the importance of focusing our political action (at all levels) on a number of key outcomes.

45. Firstly, there is a need to incorporate security as an essential design feature. The “security by design” principle is crucial for the main internet architecture and computer infrastructure of essential services, in order to reinforce the resilience vis-à-vis various forms of criminal or terroristic assaults, but also to reduce the risk and potential consequences of breakdowns. In this respect, I would commend the approach which is promoted within the European Union by Directive (EU) 2016/1148 on security of network and information systems (NIS Directive) which is aimed at achieving a high level of security of network and information systems across the European Union, through: improved cybersecurity capabilities at national level; increased EU-level co-operation; and risk management and incident reporting obligations for operators of essential services and digital service providers.[34] This approach should be encouraged in all Council of Europe member States and, possibly, expertise acquired by the European Union and its members could be shared within the wider European framework and beyond.

46. The “security by design” principle is also crucial for the network of physical devices, home appliances and other items which we call “the internet of things” (IoT) which is progressively entering into our everyday lives. The commercial interest of business companies to maximise economic benefits (and maybe the interest of governments to grasp the immediate benefit in terms of job opportunities and fiscal revenues that this business entails) cannot prevail over users’ security. It is a responsibility for developers and vendors to deliver the safest products and this responsibility should also be clearly embedded in national regulations when it comes to the IoT. For these regulations to be effective, they should be harmonised; therefore there is a need to develop harmonised international security standards; certification should become mandatory and a certification mechanism should be agreed upon. It is equally the responsibility for both private businesses and

[32] See the text in English here.

[33] See for example the reports and adopted texts on: Violent and extreme pornography; The protection of privacy and personal data on the Internet and online media; Violence in and through the media; Ending cyberdiscrimination and online hate.

Concerning cybercrime, cyberterrorism and cyberwarfare, I refer to the Assembly’s work on: Increasing co-operation against cyberterrorism and other large-scale attacks on the Internet; Improving user protection and security in cyberspace; Legal challenges related to hybrid war and human rights obligations:

[34] For further information, see the European Commission Fact Sheet.

public authorities to ensure that damage is covered; here, compulsory insurance schemes (to be entirely financed by the business sector) similar to what exists for car accidents should be introduced to mutualise risks.

47. Secondly, the struggle for security (and namely the fear of terrorist attacks and cyberwarfare and the attempt to counter these threats) is closely linked with the trend towards balkanisation of the cyberspace. While we shall reinforce domestic protection, we shall also avoid splitting the internet and establishing pervasive State control on the information flow therein. Not only will this significantly reduce internet potential, but it would also be a major threat to citizens' fundamental rights. However, what are the alternatives to balkanisation and State control which could preserve a free internet and a high level of security? I do not have a fully-fledged reply to this question, but what I would suggest is exploring the possibility to reinforce international co-operation, at least at regional level, instead of dividing ourselves, also bearing in mind that, in a global internet world, measures that are only national are very often useless.

48. There are, I believe, two main interconnected reasons that hamper stronger collaboration at international level (and even a discussion on what would be the required structures and mechanisms): the wish to remain or become predominant or at least sufficiently influential (in terms of political, military and economic powers); and the lack of trust in each other's good will and intentions. Thus, the challenge is to find the pathway that will strengthen solidarity and mutual confidence, including the will to mutualise (at least to a certain extent) domestic technology developed to enhance security. I would like to add that the aim of any attempt to reinforce international co-operation cannot be the establishment of a superstructure which will have full control instead of individual States: I fear this would be the start of an Orwellian world. I will return to this when discussing internet governance decision-making processes.

49. Thirdly, internet security is certainly a responsibility for the business sector and of public authorities; but users also have a crucial role to play. The internet community is not only the potential victim, but also the potential army against threats to individual and collective security. Therefore, their awareness of various risks, understanding on what they should do to reduce them and ability to react when they become targets of attacks or detect attacks to others are pivotal to any effective defensive strategy. Both public authorities and social media should be active in educating and training this army. This is the subject of the ongoing committee work on "Media education in the new media environment", to which I refer. However, I wish to stress here that children 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.

50. Fourthly, I believe 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. In this respect, we should call Council of Europe member States to:

– 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;

– 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;

– 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"), following the recommendations in the "Mapping study on cyberviolence" adopted by the Cybercrime Convention Committee (T-CY) on 9 July 2018;

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

51. Last but not least, Artificial Intelligence (AI) is already in the battlefield. Progress in the development of AI and of "deep learning" capacity could provide us with new robust defensive tools; but at the same time this will provide potential offenders with new powerful weapons. In addition, the possibility that in some years there could be forms of AI capable of a kind of "self-determination" raises – among others – a new kind of security issue. Our future in co-habitation with AI is a sensitive and very complex question, which I believe would deserve a new specific report.

2.5. Protection of privacy and personal data in the cyberspace

52. The technologies that are now so much part of our daily lives that they have become indispensable, and which we also use to build our interpersonal relations and to which, without giving it too much thought, little by little we entrust the most intimate aspects of our identity, are becoming a means of manipulating opinions and enabling insidious checks on our private lives.[35] This question has also been the subject of previous reports produced by the Assembly,[36] which has expressed its concern at the mass collection of personal data by private companies and has highlighted the problems associated with the creation of internet user profiles, and at the risks resulting from the actions of hackers who penetrate computer systems to obtain data held by businesses, financial institutions, research institutes and government agencies. The Assembly has also underlined 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.

53. I believe this is a domain where business interests are still prevailing on internet users' protection, notwithstanding the enhanced protection of personal data within the European Union, thanks to the General Data Protection Regulation (GDPR) now in force,[37] and the improvements in the wider European framework with the recent adoption of the Modernised Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Modernised Convention 108") which is now open for signature and ratification.[38]

54. The foreword of the new Handbook on European data protection law[39] states that "Europe is at the forefront of data protection worldwide". However, as a matter of fact, the present business model of the biggest internet operators is based on data, the new "oil" of the digital society; and (consistent with their real interest) they are all acting to get the required "user consent" for them to collect and use as they deem fit the widest possible number of (personal) data. This question is also examined in the framework of the report of our committee on "Social media: social threads or threats to fundamental freedoms?", to which I refer the reader.

3. Enhancing decision-making on internet issues

55. The question of the internet decision-making process arises at both multilateral (global or regional) level and national level, in terms of the domestic legal system. The key principles referred to over and over again in the statements of Council of Europe bodies and of other partners are applicable at all levels of decision-making, although their implementation must be context-specific. I would add that, as pointed out in the introduction, the aim is not to establish a universal model because internet governance is not monolithic but complex, with different roles and responsibilities for different stakeholders in different areas.[40] My remarks must therefore be seen as an attempt to chart the way forward for governance aimed at the actual protection of the rights identified above.

56. The Declaration by the Committee of Ministers on Internet governance principles enshrines three principles concerning decision-making which should be underlined: "multi-stakeholder governance"; "empowerment of internet users"; and "decentralised management".

[35] See, for example, Resolution 1970 (2014) "Internet and politics: the impact of new information and communication technology on democracy".

[36] See for example the reports and texts adopted on "The protection of privacy and personal data on the Internet and online media" and on "Mass surveillance".

[37] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). For more information on this regulation, see the official EC webpage on the 2018 reform of EU data protection rules and the GDPR Portal.

[38] The Modernised Convention 108 was adopted at the 128th Session of the Committee of Ministers of the Council of Europe (Elsinore, Denmark, 17-18 May 2018). For more information, see the Council of Europe webpage on the modernisation of Convention 108 and the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223).

[39] The handbook (2018 edition, at present available in English only) has been prepared by the European Union Agency for Fundamental Rights (FRA), with the Council of Europe (including the Registry of the European Court of Human Rights) and the European Data Protection Supervisor.

[40] In some areas, such as the development of core internet standards and the management of the Domain Name System, governments do not have the lead responsibility and governance is based on a multi-stakeholder approach, with private actors in the lead (IETF, ICANN, etc.).

57. The final NETmundial Multistakeholder Statement of 2014 identifies a number of “internet governance process principles”, which cover decision-making processes and the structure of decision-making bodies. Some of these principles either overlap or complement one another, while others focus more on the aims of the decision-making process than on the process itself, but essentially the three principles mentioned above are confirmed.

58. According to this Statement, internet governance should be:

– “multi-stakeholder”, “open, participative and consensus driven”, “inclusive and equitable”;

– “distributed”, i.e. “carried out through a distributed, decentralised and multi-stakeholder ecosystem;

– “enabling meaningful participation” (which requires support capacity building for the less experienced or underrepresented stakeholders).

59. The NETmundial Statement underlines that internet governance should also be “transparent”, “accountable” and “collaborative”. Transparency and responsibility are key words that appear both in the Declaration on Internet governance principles and in the texts explaining the principles of multi-stakeholder governance and decentralised management. However, I think it is worth giving them greater emphasis.

60. Good internet governance should therefore be (among other things) multi-stakeholder and decentralised, transparent and responsible, collaborative and participatory. To some extent, these principles are interconnected and support one another. For instance: in order to have an inclusive process that is also open to users, it is necessary to promote their empowerment; for all stakeholders to be able to fully play their role in multi-stakeholder governance, there is also a need to retain decentralised management. However, in order to guarantee fundamental rights, this form of management must be transparent and responsible. Accordingly, although these principles must be analysed separately, it is important not to lose sight of the links that hold them together.

3.1. Multi-stakeholder and decentralised governance, and multi-stakeholder policy dialogue on internet governance

61. There is no common definition of what a multi-stakeholder approach to internet governance could or should be.

62. To explain the “multi-stakeholder governance”, the Declaration by the Committee of Ministers of the Council of Europe on Internet governance principles speaks about the full participation of governments, the private sector, civil society, the technical community and users, taking into account their specific roles and responsibilities, and it adds that the development of international internet-related public policies and internet governance arrangements should enable full and equal participation of all stakeholders from all countries.

63. The NETmundial Statement advocates for a governance open to all stakeholders wishing to participate and ensuring their meaningful and accountable participation; it explains that the respective roles and responsibilities of stakeholders should be interpreted in a flexible manner with reference to the issue under discussion, then it adds that the development of international internet-related public policies and internet governance arrangements should enable the full and balanced participation of all stakeholders, and be made by consensus, to the fullest extent possible.

64. On this basis, multi-stakeholder governance initially involves:

– the tendentially open nature of the decision-making process, so as to be able to include all interested parties, whether governments (or, more generally, public authorities), the private sector, civil society, the technical community or users;

– participation of these parties in varying ways depending on their specific role in relation to the issues being addressed;

– in the multilateral context, the balanced, if not equal, access for stakeholders from all countries and, as far as possible, an attempt to find consensual solutions.

65. Nonetheless, several problems remain. One is the fact that, in many areas of internet governance, there is no agreement about what the respective roles and responsibilities of the different stakeholders should be. Another open question is how to ensure the qualitatively satisfactory and quantitatively fair representation of the various categories of stakeholder, given the number of potential partners and the fact that it is in

practice impossible to involve everybody (for example, all users), and how to avoid deadlock while at the same time seeking the broadest consensus, in view of the conflicting interests that may exist between, or even within, these categories of stakeholder. I have no magic solution in this connection.

66. The NETmundial Statement highlights some issues that deserve attention in the future evolution of internet governance. Two of them sound particularly relevant to me:

– stakeholder representatives appointed to a multi-stakeholder internet governance process should be selected through open, democratic and transparent procedures; different stakeholder groups should self-manage their processes based on inclusive, publicly known, well defined and accountable mechanisms;

– multi-stakeholder mechanisms should be developed at the national level, as a good portion of internet governance issues should be tackled at this level; those mechanisms should serve as a link between local discussions and regional and global instances and a fluent co-ordination and dialogue across those different dimensions is essential.

67. With regard to the first point, we could 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. As far as the second point is concerned, the aim is to 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).

68. In this respect, I would like to welcome the development of National and Regional Internet Governance Forum Initiatives (NRIs) as an integral part of the United Nations Internet Governance Forum (IGF) process.[41] The IGF and the NRIs have the potential to uphold multi-stakeholder, inclusive and collaborative approaches to internet policy design and effective implementation. They do not take decisions; they are platforms for open and inclusive multi-stakeholder dialogue. This dialogue helps in identifying opportunities and challenges that new digital technologies and internet applications bring about; it is also fundamental to building a shared understanding of stakeholders' respective roles and responsibilities. The IGF and NRIs can serve as a catalyst to identify practical solutions and foster partnerships; through setting the agenda of the discussion about public policy issues, they can influence the decision-making in other fora and institutions. Taking a closer look at the European experience, the European Dialogue on Internet Governance (EuroDIG)[42] is considered to be one of the most innovative models of democratic, bottom-up, multi-stakeholder processes among the NRIs. The Council of Europe, the European Commission and other institutions support the pan-European dialogue through their participation in the bottom-up programme planning process, without "taking over" or undermining the EuroDIG multi-stakeholder character. However, the potential of the EuroDIG, as well as of the IGF and other NRIs, is not yet fully exploited.

69. A key issue is weak funding of these fora. Like the IGF and many NRIs, EuroDIG is a fragile process, dependent on voluntary funding and on mainly voluntary resources to drive the process. A stronger presence of, and support by, the Council of Europe would help stabilise the process and guarantee a minimum level of geographical representation in EuroDIG. Another challenge is the somewhat contradictory attitude of some governments and many business representatives that insist on the IGF and NRIs remaining dialogue platforms, with no negotiations or no decisions taken, but at the same time refuse high-level participation or financial support precisely because these fora are not taking decisions and are thus not producing a "tangible outcome". Therefore, the link between the discussions in these fora and these decision-making bodies is still not strong enough.

70. At the global level, the hosts of the IGF 2017 (Switzerland), 2018 (France) and 2019 (Germany) have engaged in joint efforts to create a more tangible outcome by taking over the example of EuroDIG that since 2008 is producing a set of easy-to-read political but non-negotiated "Messages" mirroring the key findings of the debates. Furthermore, Switzerland and France have raised the political profile of the IGF with the presence of their presidents at the IGF. Another way to strengthen the political impact of the IGF, EuroDIG and the other NRIs, would be to involve more parliamentarians in the dialogue. While the number of members of the European Parliament participating at the IGF has increased over the last years, only a few members of

[41] This development also brought to the establishment of the Internet Governance Forum Support Association (IGFSA) in 2014. The purpose of the Association is to promote and support the global IGF as well as the national and regional IGF initiatives.

[42] EuroDIG is the oldest and largest regional internet governance forum. It was launched with the support of the Council of Europe in October 2008, in Strasbourg. It also counts on the institutional partnership of the European Commission and other organisations, including, for example, the European Broadcasting Union (EBU), ICANN and the Internet Society (ISOC).

national parliaments participate. I hope that our Assembly can encourage the participation of parliamentarians in national and regional IGF to help link the discussions therein with decisions to be taken at national level. With a stronger parliamentary dimension, EuroDIG could foster inter-sessional work, seeking to enhance the results of the annual event and continue the debate throughout the year, and could help strengthen the national initiatives that exist in almost every European country.

71. The Council of Europe and other stakeholders are considering how to increase effectiveness of the EuroDIG process; therefore, it might be premature to put forward concrete proposals in this respect. However, the IGF, the EuroDIG and the other NRIs are important catalysts for the implementation of recommendations adopted by the Committee of Ministers in the field of internet governance.

72. I would like to add here that inclusion at national but also European and global levels must be understood not only in terms of stakeholder groups, but also in terms of demographic diversity – i.e. a balanced representation of gender, age and also ethnicity, as appropriate. In this respect, it seems that there is still quite a long way to go. Therefore, when encouraging the establishment of multi-stakeholder platforms to discuss internet governance at State level, I would suggest paying more attention to this dimension of their inclusiveness.

73. As far as decentralisation is concerned, the idea resulting from the Declaration on Internet governance principles is to maintain the current situation, in which organisations tasked with technical aspects and aspects of internet management,[43] as well as the private sector, have a key technical and operational role to play. The aim, therefore, is not to concentrate powers exclusively in the hands of States (and intergovernmental organisations).

74. However, I believe that the decentralisation principle involves something else too and that it should be understood as being inextricably linked to the idea of (context-specific) “subsidiarity”: internet governance (like any governance of social networks) requires us 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.

75. Understood in this way, the idea of decentralised internet governance not only calls for the vertical distribution of powers (by highlighting the existence of decision-making centres at various levels) but also their horizontal distribution among players of different kinds. In this sense, decentralised and multi-stakeholder governance go hand in hand.

3.2. Transparent and accountable governance

76. The Declaration on Internet governance principles, when encouraging decentralised management of the internet, also states that “[t]he bodies responsible for the technical and management aspects of the Internet, as well as the private sector should retain their leading role in technical and operational matters while ensuring transparency and being accountable to the global community for those actions which have an impact on public policy”. We could say, more generally, that all those participating in internet governance should ensure transparency of their actions and should be accountable.

77. According to the NETmundial Statement, transparent internet governance requires that decisions made must be easy to understand, and processes must be clearly documented and procedures followed which have been developed and agreed upon through multi-stakeholder processes.

78. Transparency first and foremost requires us to have a precise understanding of who decides what. This aspect does not appear directly in the definition contained in the NETmundial Statement, perhaps because the problem typical of the actual concept of governance in general lies in the difficulty in establishing the exact location of a “decision-making centre”, on account of the fragmentation of decision-making power. This is not the place to discuss this problem in any depth. To simplify matters, I believe that it must be possible even in a complex multi-stakeholder decision-making process to identify each stakeholder’s responsibility with regard to the final decision (and its implementation). It is not possible to abandon this principle without at the same time abandoning every thought of the legitimacy of decision makers and of democratic oversight, and thereby paving the way for behind-the-scenes players and survival of the fittest.

[43] For example: the Internet Corporation for Assigned Names and Numbers (ICANN), the Regional Internet Registries (RIRs) or the Internet Engineering Task Force (IETF).

79. To some extent, the question can be covered by the requirement that the decision-making process (and therefore the intervention of each party) should follow a clearly established procedure. The NETmundial Statement adds that the procedures in question should be built on multi-stakeholder processes. It may be impossible in practice to follow this through to its logical conclusion as it will then be necessary to legitimise these multi-stakeholder processes and establish the corresponding procedures which must then be agreed; and so on and so forth. I therefore think that the community of States (and, in the domestic context, the legislature) should be given a leading role here. This approach is no doubt justified in the case of decision-making processes that have an (actual or potential) impact on human rights.

80. Internet governance requires clearer procedures, which must be laid down by the community of States in consultation with other stakeholders in accordance with a multi-stakeholder approach. At European level, the Council of Europe and the European Union are the bodies that should act together and take up this challenge.

81. Finally, transparency presupposes that the meaning of decisions taken should be comprehensible for those affected by them and that these decisions are made public – and are therefore documented, categorised and published in such a way as to be easily available to everyone. In this connection, the dispersal of decision-making centres makes a form of “centralisation” necessary, and consideration should be given to a common system of information on internet governance.

82. Transparency is the best antidote we have to curb arbitrary action and the insidious predominance of vested interests (including State interests) over the public good. It is also the essential precondition of responsible governance.

83. Concerning “accountability”, the NETmundial Statement advocates the setting up of mechanisms for independent checks and balances as well as for review and redress; and it states that, “in this respect, governments have primary, legal and political accountability for the protection of human rights”.

84. We are fully aware of the strengths and weaknesses of independent oversight, review and redress mechanisms to ensure respect for human rights at both international and European level. An analysis of their effectiveness in the case of violations of the rights discussed in section 2 (and other rights that may be called into question on and through the internet) is outside the scope of this report. Similarly, it is not possible to consider here the question of the effectiveness of the protection provided at national level, given the cross-border dimension of the internet (with all its many problems associated with the jurisdiction of the domestic courts, the law that is applicable and the enforcement of judgments).

85. I would nonetheless like to draw attention to the difficulty in ensuring genuine transparency and the effective oversight of the actions of the major private internet operators and also point out that it is sometimes governments themselves that are responsible for human rights violations, as in the case of mass surveillance operations or cyberwarfare.

86. With regard to the latter, I wonder whether it would be possible to strengthen the existing forms of co-operation and, perhaps, create a specific monitoring mechanism and establish crisis management and post-crisis analysis by sharing resources that already exist in various countries. In the case of the European Union, the European Commission has suggested reinforcing the European Union Agency for Network and Information Security (ENISA),[44] which could become a full-blown European cybersecurity agency. As far as the Council of Europe is concerned, a possible model could be the EUR-OPA Major Hazards Agreement.[45] I am aware that such co-operation calls for a high level of mutual trust and that it is sometimes precisely that trust that is lacking. However, I am also aware that gradually building forms of co-operation on sensitive matters is probably the most effective means of increasing the mutual trust we need so much.

[44] ENISA is a centre of expertise for cyber security in Europe, which helps the European Union and EU countries to be better equipped and prepared to prevent, detect and respond to information security problems.

[45] EUR-OPA Major Hazards Agreement is a platform for co-operation between Europe and the South of the Mediterranean in the field of major natural and technological disasters. Its field of competence covers disaster risk reduction, in particular knowledge, prevention, preparedness, risk management and post-crisis analysis. Its main objectives are to reinforce and to promote co-operation between member States in a multi-disciplinary context to ensure better prevention, protection against risks and better preparation in the event of major natural or technological disasters.

3.3. Collaborative and participatory governance

87. The NETmundial Statement calls for a collaborative internet governance, based on co-operative approaches that reflect the inputs and interests of stakeholders. The Declaration on Internet governance principles underlines that "[i]n order to preserve the integrity and ongoing functioning of the Internet infrastructure, as well as users' trust and reliance on the Internet, it is necessary to promote national and international multi-stakeholder co-operation".

88. Co-operation calls for stakeholders to have a positive attitude in two areas: firstly, the recognition of the role of the other parties and of the added value that the contribution of each of them provides; and secondly a commitment to place one's own expertise, skills and resources at the service of the common good. Multi-stakeholder internet governance makes sense only if the parties are driven by this collaborative spirit. The danger to be avoided is that a willingness to participate is expressed with the sole aim of protecting one's own interests without caring too much about those of other stakeholders.

89. I am not so naive as to believe that stakeholders will cease to defend their own particular interests. To a certain extent, it is quite normal for them to do so. In a multi-stakeholder context, it is natural for there to be some conflict between the interests of the various bodies, so it is also necessary to focus on how representative they are. Co-operation does not mean abandoning one's own interests, but involves accepting that common goals take precedence and that it is not always possible to fully reconcile co-operation with gains sought individually.

90. Concerning participation, the Declaration on Internet governance principles speaks about the "empowerment of internet users" and states that "[u]sers should be fully empowered to exercise their fundamental rights and freedoms, make informed decisions and participate in Internet governance arrangements, in particular in governance mechanisms and in the development of Internet-related public policy, in full confidence and freedom". The NETmundial Statement calls for a meaningful participation of different stakeholders. To this aim "internet governance institutions and processes should support capacity building for newcomers, especially stakeholders from developing countries and underrepresented groups".

91. Participation complements both the collaborative and the multi-stakeholder aspects: it presupposes not only openness to the partners concerned – and in particular to users – but also a proactive attitude and a commitment to provide them with the means of participating to enable them to be meaningfully involved.

92. The subject of empowering users so that they can in practice participate in internet governance falls within the scope of two reports currently being drafted by our committee, on the role of education in the digital era and on media education in the new media environment. I will therefore simply make the point here that one of the shortcomings of current internet governance is that, *de facto,* it involves only "insiders". The challenge is therefore to move beyond the circle of professionals in this field and ensure that experts in other fields can contribute to the development of the internet. This is all the more essential given that the internet (as we have emphasised) has an impact on all aspects of our societies (political, legal, economic, social, cultural and ethical).

4. Conclusions

93. The internet has profoundly changed our society and continues to do so. It has enormous potential and is a key instrument for enabling individuals to exercise their rights to freedom of opinion and expression, as well as other fundamental rights, and for promoting progress. However, it can also be used to destroy the values we hold dear, so we need to manage its development more effectively in order to avoid this.

94. Indeed, shaping the internet is also shaping a global society and setting the path of its development, and, to a significant extent, of the progress of our national societies. Therefore, internet governance should be a priority for policy makers. Our aim should be to ensure that public policy for internet is people-centred and respects the core values of democracy, human rights and the rule of law.

95. The concern for human rights must inform the definition of key objectives of internet governance and the role and responsibilities of different stakeholders. Institutional arrangements and decision-making processes, as well as the regulatory framework of the internet and the mechanisms established to monitor compliance with the norms and rules therein, must be designed to ensure that human rights are truly recognised and effectively guaranteed.

96. My analysis points to some challenges that internet governance has to face concerning human rights. We need to reach a common understanding of the scope of the human rights in question, which, notwithstanding their proclaimed "universality", are not perceived and implemented uniformly. We need to

enhance protection of these rights against threats from States and from private actors. We also need to reduce gaps in enjoyment of these rights and, to begin with, elaborate concrete policies and action plans to fill in the “digital gap”. Finally, we need to solve potential tensions between different rights.

97. Similarly, I have identified some challenges concerning internet governance processes, such as: avoiding the danger that the internet and the global internet community itself become splintered; enhancing the effectiveness of multi-stakeholder and multilevel decision-making; better co-ordinating top-down and bottom-up governance processes, by balancing and possibly reconciling the diverse interests of various key stake-holders.

98. With regard to the protection in the practice of fundamental rights, public authorities have a key role to play and have non-transferable responsibilities. Therefore, although I advocate a multi-stakeholder internet governance model, in my view it would not be desirable to opt for a multi-stakeholder governance model that would water down States’ responsibilities in the field of promoting and safeguarding fundamental rights.

99. Governments and national parliaments remain the decision makers with regard to citizens’ rights (and duties) and are responsible for ensuring their effectiveness. In the area of internet governance, while being open to dialogue and respecting the role of other stakeholders, public authorities have a duty to launch the appropriate initiatives to establish standards, oversight mechanisms and measures required when violations occur. It is not enough to simply reassert this role and responsibility; we need to work together to ensure that this is properly carried out. For this reason, I believe it is essential to intensify international co-operation.

100. In this respect, internet governance is a domain where the Council of Europe can bring quite significant “added value”; thus I hope that short-sighted financial considerations can be overcome by a wiser approach, maybe in the form of a specific programme founded by earmarked voluntary contributions, or even the launching of a new enlarged partial agreement on “internet governance”.

101. Last but not least, we parliamentarians should become more aware of the actual and potential huge impact that decision-making in the field of internet and cyberspace has on our lives as individuals and as societies, including in the effectiveness and resilience of our democratic system. We should also be more proactive both within the domestic sphere, as legislature, in the definition of comprehensive internet strategies, and in encouraging our governments to act collectively through the intergovernmental organisations in internet governance multilateral decision-making processes.

102. To this end, we have at our disposal the many well-thought-out recommendations adopted by the Committee of Ministers, of which we should make better use. We now also have the UNESCO “Internet Universality Indicators” (released on 17 October 2018)[46] through which we could assess levels of achievement in our countries by the four ROAM fundamental principles included in the concept of “Internet Universality”, which means that the internet should be: based on human rights (R), open (O), accessible to all (A) and nurtured by multi-stakeholder participation (M)

[46] See: https://en.unesco.org/internetuniversality/indicators.