DEFENDING FREEDOM
OF EXPRESSION AND INFORMATION

ARTICLE 19 Free Word Centre 60 Farringdon Road London EC1R 3GA
T +44 20 7324 2500 F +44 20 7490 0566
E info@article19.org W www.article19.org Tw @article19org facebook.com/article19org

ARTICLE 19

Freedom of expression and ICTs: Overview of international standards

2013

ARTICLE 19
Free Word Centre
60 Farringdon Road
London
EC1R 3GA
United Kingdom
T: +44 20 7324 2500
F: +44 20 7490 0566
E: info@article19.org
W: www.article19.org
Tw: @article19org
Fb: facebook.com/article19org

ISBN: 978-1-906586-67-6

This document has been published with support of the Adessium Foundation of The Netherlands, as part of their wider support for ARTICLE 19's work on freedom of expression and internet communications technology.

Table of contents

Introduction 3

International standards on freedom of expression and ICTs 5

- The founding principles of freedom of expression 6
- Limitations on the right to freedom of expression 7
- Regional standards 8

Access to the internet 12

- Universal access to the internet 13
- Net neutrality 14
- Three-strikes and disconnection 15

Controlling access to online content 16

- Blocking, filtering and removing content 17
- Domain name seizure or suspension 18
- Intermediary liability/liability for third-party content 19
- Linking liability 21

Online content regulation 23

- Cybercrime 25

The rights of citizen journalists and bloggers 27

- Definition of journalism and new media 28
- Regulation of bloggers and citizen journalists 29

Access to information and ICTs 31

- E-governance and e-government 32
- Open data 33

Regulatory framework of the internet 35

- Internet governance 36
- Jurisdiction 38

Acknowledgements

ARTICLE 19 is an international human rights organisation, founded in 1987, which defends and promotes freedom of expression and freedom of information worldwide. It takes its mandate from the Universal Declaration of Human Rights, which guarantees the right to freedom of expression and information. An increasingly important means to express oneself and to seek, receive and impart information is through information and communication technologies such as the internet. Hence, ARTICLE 19 has been promoting the internet freedoms for over 10 years and is active in developments in policy and practice around freedom of expression and the internet through our network of partners, associates and expert contacts. We have also analysed various internet related laws, including those in Brazil, Bolivia, Russia, Pakistan, Iran, Iraq, UK, Tunisia, and Venezuela.

This report is published with the support of the Adessium Foundation of The Netherlands, as part of their wider support for ARTICLE 19's work on freedom of expression and internet communications technology.

Introduction

The internet and new information communication technologies (ICTs) are now an integral part of everyday life for many people around the world. ICTs are giving more and more people a voice and are improving openness and public debate in the society.

At the same time, restrictions on the right to freedom of expression in relation to ICTs are on the increase: there have been many warnings that more and more states are trying to increase their grip on the growing flow of data and how people express themselves online.[1] More and more, it is private actors and international corporations who are the providers and enablers of ICTs and who therefore make the decisions about the extent to which citizens are able to enjoy the right to freedom of expression.

In various discussions about the protection of freedom of expression and ICTs, a question has emerged asking whether the internet needs a separate set of international laws and treaties specifically designed for the new medium or whether legal issues pertaining to the web should be tackled within existing legislation and international standards.

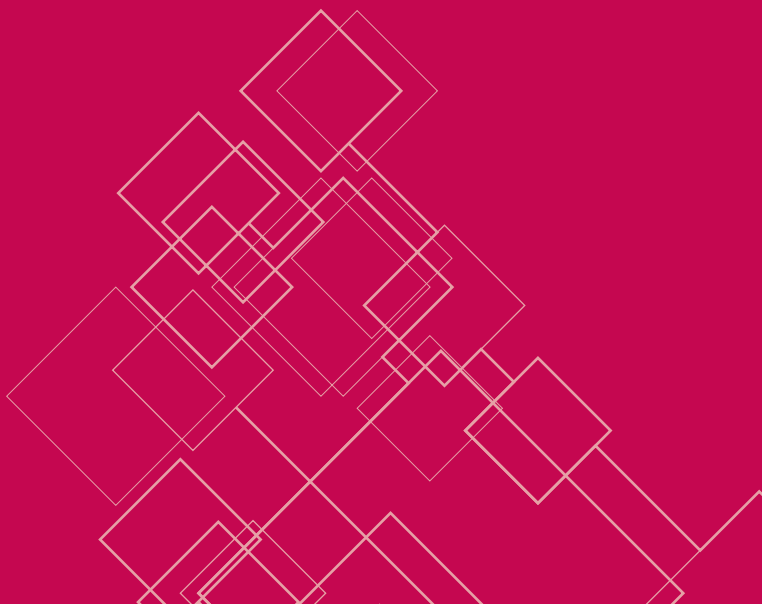
The former suggestion is based on the assumption that the global and decentralised flow of information on the internet and in cyberspace as a whole cannot be linked to a particular jurisdiction or sovereign state. Furthermore, it is argued that the enforcement of existing laws can barely keep up with the volume of data flow, the increase in cybercrime and attacks to the internet's infrastructure. The latter suggestion, supported by many international human rights organisations, is based on the presumption that the internet is merely another platform for communication and not a separate virtual world: thus existing legal standards apply. Existing legal rules on particular issues (e.g. copyright, defamation and privacy rights) are likely to need adapting to reflect the nature and pace of the digital age; however, given the fear that the internet causes some governments around the world, new international standards bear the risk of watering down existing human rights standards and of fragmenting and 'nationalising' the internet.

ARTICLE 19 argues that the right to freedom of expression was not designed to fit any particular medium or technology. Regardless of whether it is exercised online or offline, it is an internationally protected right to which almost all countries of the world have committed themselves.

This publication provides an overview of the main international standards relevant to the protection of the right to freedom of expression in relation to ICTs. It identifies international and regional standards for the protection of key areas of concern, in particular access to the internet and controlling access to online content, content regulation, the rights of citizen journalists and bloggers, access to information and ICTs and the regulatory framework of the internet.

It is intended as a resource for anyone with an interest in promoting the realisation of the right to freedom of expression on the internet, such as journalists, public officials, judges, lawyers and civil society campaigners.

International standards on freedom of expression and ICTs



The founding principles of freedom of expression

Article 19 of the Universal Declaration of Human Rights (UDHR)[2] guarantees the right to freedom of expression in the following terms:

> Everyone has the right to freedom of opinion and expression; this right includes the right to hold opinions without interference and to seek, receive, and impart information and ideas through any media and regardless of frontiers.

The UDHR, as a UN General Assembly Resolution, is not directly binding on states. However, parts of it, including Article 19, are widely regarded as having acquired legal force as customary international law since it was adopted in 1948.[3]

The International Covenant on Civil and Political Rights (ICCPR) elaborates upon and gives legal force to many of the rights articulated in the UDHR.[4] It guarantees the right to freedom of expression in terms similar to those of Article 19 of the UDHR:

1 Everyone shall have the right to freedom of opinion

2 Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art or through any other media of his choice.

In September 2011, the UN Human Rights Committee (HR Committee), a treaty monitoring body for the ICCPR, issued General Comment No 34 in relation to Article 19.[5] General Comment No.34 constitutes an authoritative interpretation of the minimum standards guaranteed by Article 19 of the ICCPR. It is particularly instructive about a number of issues relating to freedom of expression on the internet.

Importantly, General Comment No.34 states that Article 19 of the ICCPR protects all forms of expression and the means of their dissemination, including all forms of electronic and internet-based modes of expression.[6] In other words, the protection of freedom of expression applies online in the same way as it applies offline.

At the same time, General Comment No.34 requires States party to the ICCPR to consider the extent to which developments in information technology, such as internet and mobile-based electronic information dissemination systems, have dramatically changed communication practices around the world.[7] In particular, it states that the legal framework regulating the mass media should take into account the differences between print and broadcast media and the internet, as well as noting the ways in which the various media converge.[8]

Further, in June 2012, the Human Rights Council unanimously adopted the landmark Resolution on the promotion, protection and enjoyment of human rights on the internet, affirming:

> That the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.[9]

Earlier, in May 2011, in his report to the UN Human Rights Council, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, underscored that:

> Article 19 of the Universal Declaration of Human Rights and the Covenant was drafted with foresight to include and to accommodate future technological developments through which individuals can exercise their right to freedom of expression. Hence, the framework of international human rights law remains relevant today and equally applicable to new communication technologies such as the internet.[10]

Similarly, the four special mandates for the protection of freedom of expression have highlighted in their Joint Declaration on Freedom of Expression and the internet of June 2011[11] that regulatory approaches in the telecommunications and broadcasting sectors cannot simply be transferred to the internet. In particular, they recommend the development of tailored approaches for responding to illegal content online, as well as pointing out that specific restrictions for material disseminated over the internet are unnecessary.[12] They also promote the use of self-regulation as an effective tool in redressing harmful speech.[13]

Limitations on the right to freedom of expression

While the right to freedom of expression is a fundamental right, it is not guaranteed in absolute terms.

Article 19(3) of the ICCPR permits the right to be restricted in the following respects:

> The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
>
> (a) For respect of the rights or reputations of others;
>
> (b) For the protection of national security or of public order, or of public health or morals.

Restrictions on the right to freedom of expression must be strictly and narrowly tailored and may not put in jeopardy the right itself. Determining whether a restriction is narrowly tailored is often articulated as a three-part test. Restrictions must: (i) be provided by law; (ii) pursue a legitimate aim; and (iii) conform to the strict tests of necessity and proportionality.[14]

– Provided by law: Article 19(3) of the ICCPR requires that restrictions on the right to freedom of expression must be provided by law. In particular, the law must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly.[15] Ambiguous or overly broad restrictions on freedom of expression are therefore not permitted under Article 19(3).

– Pursue a legitimate aim: Interferences with the right to freedom of expression must pursue a legitimate aim as exhaustively enumerated in Article 19(3)(a) and (b) of the ICCPR. As such, it would be impermissible to prohibit information dissemination systems from publishing material solely on the basis that they cast a critical view of the government or the political social system espoused by the government.[16] Similarly, a restriction on freedom of expression cannot be a pretext for protecting the government from embarrassment or exposure of wrongdoing, to conceal information about the functioning of its public institutions or to entrench a particular ideology.

– Conform to the tests of necessity and proportionality: States party to the ICCPR are obliged to ensure that any legitimate restrictions on the right to freedom of expression are necessary and proportionate. Necessity means that there must be a pressing social need for the restriction. The party invoking the restriction must show a direct and immediate connection between the expression and the protected interest. Proportionality means that the least restrictive measure must be applied if it is capable of achieving the same purpose as a more restrictive one.

The same principles apply to electronic forms of communication or expression disseminated over the internet. In particular, the UN Human Rights Committee has said in its General Comment No. 34 that:

> 43. Any restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3. Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with paragraph 3. It is also inconsistent with paragraph 3 to prohibit a site or an information dissemination system from publishing material solely on the basis that it may be critical of the government or the political social system espoused by the government.[17]

These principles have been endorsed by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, in his 2011 report. In that report, the Special Rapporteur also clarified the scope of legitimate restrictions on different types of expression online.[18]

Regional standards

A number of regional instruments also guarantee the right to freedom of expression and information.

African Charter on Human and Peoples' Rights (the African Charter)[19] guarantees the right to freedom of expression in Article 9 using the following terms:

1 Every individual shall have the right to receive information.

2 Every individual shall have the right to express and disseminate his opinions within the law.

The African Commission on Human and Peoples' Rights (the African Commission) elaborated on Article 9 of the African Charter in October 2002, adopting the Declaration of Principles on Freedom of Expression in Africa (the African Declaration):[20] In Article 1 it provides that:

1 Freedom of expression and information, including the right to seek, receive and impart information and ideas, either orally, in writing or in print, in the form of art, or through any other form of communication, including across frontiers, is a fundamental and inalienable human right and an indispensable component of democracy.

2 Everyone shall have an equal opportunity to exercise the right to freedom of expression and to access information without discrimination.

The American Declaration of the Rights and Duties of Man[21], adopted by the Organization of American States (OAS) in 1948, stipulates in Article IV that:

> Every person has the right to freedom of investigation, of opinion, and of the expression and dissemination of ideas, by any medium whatsoever.

Article 13 of the American Convention on Human Rights[22] goes further by specifying the positive obligation of states and including a ban on censorship and 'indirect' restriction:

1 Everyone has the right to freedom of thought and expression. This right includes freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing, in print, in the form of art, or through any other medium of one's choice.

2 The exercise of the right provided for in the foregoing paragraph shall not be subject to prior censorship but shall be subject to subsequent imposition of liability, which shall be expressly established by law to the extent necessary to ensure: a. respect for the rights or reputations of others; or b. the protection of national security, public order, or public health or morals.

3 The right of expression may not be restricted by indirect methods or means, such as the abuse of government or private controls over newsprint, radio broadcasting frequencies, or equipment used in the dissemination of information, or by any other means tending to impede the communication and circulation of ideas and opinions.

The Inter-American Declaration of Principles on Freedom of Expression, a basic document for interpreting Article 13 of the American Convention, makes clear reference to new technology in both the language and spirit of Principle 5:

> Prior censorship, direct or indirect interference in or pressure exerted upon any expression, opinion or information transmitted through any means of oral, written, artistic, visual or electronic communication must be prohibited by law. Restrictions to the free circulation of ideas and opinions, as well as the arbitrary imposition of information and the imposition of obstacles to the free flow of information violate the right to freedom of expression.[23]

In Asia, the ASEAN Human Rights Declaration of November 2012, which is not legally binding, follows the languages of the ICCPR in Article 23, stipulating that:

> Every person has the right to freedom of opinion and expression, including freedom to hold opinions without interference and to seek, receive and impart information, whether orally, in writing or through any other medium of that person's choice.[24]

However, the ASEAN Declaration as a whole falls below international standards on human rights.

The Arab Charter on Human Rights (Arab Charter), adopted by the Council of the League of Arab States in 2004, purports to affirm the principles of the UDHR and ICCPR, as well as the International Covenant on Economic, Social and Cultural Rights (ICESCR), the UN Charter and the Cairo Declaration on Human Rights in Islam.[25]

Although the Arab Charter provides less robust protections for certain fundamental rights, Article 32 of the Revised Arab Charter protects freedom of expression in the following terms:

1 The present Charter guarantees the right to information and to freedom of opinion and expression, as well as the right to seek, receive and impart information and ideas through any medium, regardless of geographical boundaries.

2 Such rights and freedoms shall be exercised in conformity with the fundamental values of society and shall be subject only to such limitations as are required to ensure respect for the rights or reputation of others or the protection of national security, public order and public health or morals.

It is significant that even this controversial text protects in express terms the rights to freedom of expression and freedom of information.

Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)[26] provides that:

1 Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

2 The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

In addition, Article 11 of the Charter of Fundamental Rights of the European Union (the EU Charter)[27] mainly follows the formulation of Article 19 of the ICCPR.

It should also be highlighted that at the Council of Europe, the Committee of Ministers recently adopted two recommendations relating to internet freedom: the Recommendation 'on a new notion of media'[28] and the Recommendation 'on the protection and promotion of the universality, integrity and openness of the internet.[29]

International jurisprudence and the adoption of legally binding international human rights instruments on the freedom of expression in the context of ICTs has been slow compared to the speed at which the internet has spread and developed.[30] However, the last two years have seen some important decisions by the European Court of Human Rights and the European Court of Justice.[31]

Access to the internet

Universal access to the internet

Access to the internet is crucial for the enjoyment of the right to freedom of expression and other rights in the digital age. It has been observed that without the means to connect or without an affordable connection, the right to freedom of expression and the freedom of the media become meaningless in the online world.[32]

Although it has not yet been established as a distinct human right under international law, the right to universal access to the internet has been mentioned or referred to in several documents. For example:

- The Declaration of Principles of the 2003 World Summit on the Information Society (WSIS) states that "communication is a fundamental social process, a basic human need and the foundation of all social organization. It is central to the Information Society. Everyone, everywhere should have the opportunity to participate and no one should be excluded from the benefits the Information Society offers."[33]
- General Comment No. 34 calls on states to "take all necessary steps to foster the independence of [information and communication technologies, such as internet and mobile based electronic information dissemination systems] and to ensure access of individuals thereto."[34]
- The 2011 report of the UN Special Rapporteur on freedom of expression called on states "to ensure that internet access is maintained at all times, including during times of political unrest."[35] The Special Rapporteur also differentiated between two 'dimensions' to the topic: access to online content and access to the "infrastructure and information communication technologies, such as cables, modems, computers and software, to access the internet in the first place."[36] He highlighted that access to the infrastructure and "ensuring universal access to the internet should be a priority for all States. Each State should thus develop a concrete and effective policy, in consultation with individuals from all sections of society, including the private sector and relevant Government ministries, to make the internet widely available, accessible and affordable to all segments of population."[37]
- The 2011 Joint Declaration of four special mandates on freedom of expression stressed that "states are under a positive obligation to facilitate universal access to the internet" and that "giving effect to the right to freedom of expression imposes an obligation on States to promote universal access to the internet."[38]
- Some national legislation recognises access to the internet either as a basic human right or as being implied as part of the fundamental right to freedom of expression.[39] The states that guarantee the right of access to the internet within their national legislation include Greece,[40] Estonia,[41] France,[42] Finland,[43] Spain[44] and Costa Rica.[45]

Net neutrality

An important component of the right of access to the internet is the principle of 'network neutrality' or 'net neutrality.' This protects the right to access internet content, applications, services and hardware according to individual choice. It requires that ISPs and governments treat all traffic and data on the internet equally, without discrimination, regardless of the nature of the sender, user, type of data, content, and platform. ISPs and governments are also prohibited from prioritising the transmission of data, from blocking content, or from slowing down access to certain applications or services.

A sub-category within net neutrality is 'platform neutrality', which allows users to have full access to all features and websites on the internet in the same form, regardless of the device they use to log on to the web.

Proponents of net neutrality argue that it is essential in order to guarantee the right to free expression, maintain a free flow of information and ideas and avoid the creation of artificial scarcity. On the other hand, opponents view net neutrality as having a negative impact on the quality of service since different services require different treatment for their transmission.

There has been extensive debate about whether and how net neutrality should be imposed by legislation, given that self-regulatory approaches proved to be non-workable.[46] It has been also argued that the legislation of most countries is not able to prevent discrimination against certain types of content on the internet.[47]

Net neutrality is not yet anchored as a legal norm within international law. However, the 2011 Joint Declaration on Freedom of Expression and the internet of the four Rapporteurs recommended that:

> There should be no discrimination in the treatment of internet data and traffic, based on the device, content, author, origin and/or destination of the content, service or application.
>
> Internet intermediaries should be required to be transparent about any traffic or information management practices they employ, and relevant information on such practices should be made available in a form that is accessible to all stakeholders.[48]

In Europe, there have been a few limited attempts to secure equal access for all users to online content. These have included:

– Conclusions of the Council of the EU about the open internet and net neutrality in Europe, inviting the member states to "encourage the application of the principle of net neutrality."[49]

– Non-legislative resolutions passed by the European Parliament in which it has called for transparent internet traffic management. It has also asked the European Commission to ensure that internet service providers do not block, discriminate against, impair or degrade the ability of any person to use a service to access, use, send, post, receive or offer any content, application or service of their choice, irrespective of source or target;[50] to propose legislation to ensure net neutrality[51] and codify the principle of net neutrality by means of appropriate regulation.[52]

In addition, several states have adopted national legislation on net neutrality. These include Chile,[53] the Netherlands,[54] Slovenia[55] and the USA.[56]

Three-strikes and disconnection

The so-called 'three-strikes' are protocols or laws which have been adopted in several countries,[57] aimed at reducing unlawful file-sharing. Typically, the users are sent three warnings for allegedly infringing copyright. Repeat offenders face measures such as bandwidth reduction, protocol blocking, account suspension or disconnection from the internet.

The most severe measure – disconnection from the internet – has been recently criticised as a highly disproportionate sanction as it prioritises the enforcement of copyright over the fundamental right to freedom of expression and the right to privacy. Given the fact that IP addresses cannot often be attributed to a particular user or can easily be manipulated, measures of this kind also raise concerns regarding their proportionality and the presumption of innocence. For example:

In his 2011 report, the UN Special Rapporteur considered that cutting off users from internet access, regardless of the justification provided, including on the grounds of violating intellectual property rights laws, to be disproportionate and thus a violation of the right to freedom of expression. He urged "states to repeal or amend existing intellectual copyright laws which permit users to be disconnected from internet access, and to refrain from adopting such laws."[58]

In the 2011 Joint Declaration, the four special rapporteurs on freedom of expression stated that "denying individuals the right to access the internet as a punishment is an extreme measure, which could be justified only where less restrictive measures are not available and where ordered by a court, taking into account the impact of this measure on the enjoyment of human rights."[59]

Three-strikes measures are also problematic from a human rights perspective because they require ISPs to monitor or filter their users' online behaviour which may result in an invasion of privacy. In this respect, the European Court of Justice has ruled that monitoring, filtering and blocking systems installed by ISPs or social networks for the prevention of copyright infringements are disproportionate and in breach with fundamental rights, particularly the rights to privacy and freedom of information.[60]

Controlling access to online content

Blocking, filtering and removing content

Decisions to block, filter and remove content are severe types of censorship and are popular measures used by governments, national administrations and ISPs to handle unwanted or controversial content.

These measures are often undertaken on a questionable basis in the absence of domestic legislation. Decisions to block, filter and remove content rarely follow a due process and are not necessarily taken by independent courts or adjudicatory bodies.[61] These measures are also easy to achieve as many states place hold intermediaries unduly liable. Moreover, it has been observed that blocking policies are ineffective, given the speedy reappearance and easy circumvention of blocked or filtered content, and also taking into account the financial burden of blocking systems on ISPs and consumers.[62]

Compatibility with the right to freedom of expression

The problematic nature of these measures has been addressed by the four special rapporteurs in their 2011 Joint Declaration, in which they stated that:

(a) Mandatory blocking of entire websites, IP addresses, ports, network protocols or types of use (such as social networking) is an extreme measure analogous to banning a newspaper or broadcaster. It can only be justified in accordance with international standards, for example where necessary to protect children against sexual abuse.

(b) Content filtering systems which are imposed by a government or commercial service provider and which are not controlled by the end-user are a form of prior censorship and are not justifiable as a restriction on freedom of expression.

(c) Products designed to facilitate end-user filtering should be accompanied by clear information to end-users about how they work and their potential pitfalls in terms of over-inclusive filtering.[63]

At a regional level, several European bodies have taken a position on the compatibility of these measures with human rights standards. In 2012, the European Court of Human Rights[64] ruled that blocking was compatible with the European Convention only if a strict legal framework was in place regulating its scope and affording the guarantee of judicial review to prevent possible abuses. The European Court also highlighted that the protection of the right to freedom of expression applied not only to the content of the expression but also to the means of disseminating it and that the right to freedom of expression applied "regardless of frontiers."

Due process

Lack of compliance with due process standards seems to be one of the main challenges with blocking and filtering measures. In particular, it has been pointed out that governments and ISPs take these decisions in a non-transparent manner and that efficient, timely and independent appeals procedures are largely unavailable.

The UN Special Rapporteur on freedom of expression stressed that:

> Any requests submitted to intermediaries to prevent access to certain content, or to disclose private information for strictly limited purposes such as administration of criminal justice, should be done through an order issued by a court or a competent body which is independent of any political, commercial or other unwarranted influences.[65]

At a regional level, two Council of Europe Recommendations on the protection of human rights with regard to search engines and social networking sites include provisions on due process, particularly in the context of self-regulatory mechanisms. In these recommendations, the Committee of Ministers asks member states to:

> [P]romote transparent self- and co-regulatory mechanisms for search engines, in particular with regard to the accessibility of content declared illegal by a court or competent authority, as well as of harmful content, bearing in mind the Council of Europe's standards on freedom of expression and due process rights.
>
> [E]nsure that any law, policy or individual request on de-indexing or filtering is enacted with full respect for relevant legal provisions, the right to freedom of expression and the right to seek, receive and impart information. The principles of due process and access to independent and accountable redress mechanisms should also be respected in this context.[66]

It also states that it is:

> [I]mportant that procedural safeguards are respected by these mechanisms, in line with the right to be heard and to review or appeal against decisions, including in appropriate cases the right to a fair trial, within a reasonable time, and starting with the presumption of innocence.[67]

Domain name seizure or suspension

Domain name seizure or the suspension of websites is another extreme measure which is problematic from a human rights perspective. While the consequences of domain name blocking are restricted to a particular jurisdiction and state, domain name seizure affects respective content worldwide. The main concerns about the compatibility of these measures with human rights standards include the disproportionate nature of these measures: while domain name seizure might pursue a legitimate aim, for example to protect children and minors, it often leads to blocking legitimate content.[68]

In addition, measures are implemented in the absence of due process guarantees, with little or no judicial oversight. It has been observed that court orders permitting domain name seizures are made on the basis of ex parte affidavits, meaning that only the government presents evidence and website operators have no opportunity to be heard or to respond to allegations until their websites have been shut down.[69]

Intermediary liability/liability for third-party content

Internet intermediaries – such as internet service providers, search engines and social media platforms – play a crucial role in enabling people around the world to communicate with each other. Because of their technical capabilities, internet intermediaries are under increasing pressure from governments and interest groups to police online content.

Using a variety of methods,[70] a growing number of governments have started to enlist - and in some cases compel - intermediaries in removing or blocking citizens' access to content which they deem illegal or "harmful."[71] While some of these restrictions are applied directly by a state regulator,[72] many states have adopted legal regimes for civil liability that have effectively forced internet intermediaries to police aspects of the internet on the state's behalf.[73]

Imposing intermediary liability on ISPs is problematic from a freedom of expression perspective. Primarily, it gives intermediaries quasi-judicial authority to decide about the legality of content. However, intermediaries are not only ill-equipped and lacking the legitimacy to pursue such a role, they are also not required to follow due process procedures, to make their decisions transparent or to offer independent appeals mechanisms.

In his 2011 report, the UN Special Rapporteur on freedom of expression criticised such intermediary liability systems, pointing to the lack of appeals mechanisms, the risk of self-censorship of intermediaries and the fact that private bodies are ill-placed to balance the different fundamental rights when taking decisions on content removal:

> [W]hile a notice-and-takedown system is one way to prevent intermediaries from actively engaging in or encouraging unlawful behaviour on their services, it is subject to abuse by both State and private actors. Users who are notified by the service provider that their content has been flagged as unlawful often have little recourse or few resources to challenge the takedown. Moreover, given that intermediaries may still be held financially or in some cases criminally liable if they do not remove content upon receipt of notification by users regarding unlawful content, they are inclined to err on the side of safety by over-censoring potentially illegal content. … Furthermore, intermediaries, as private entities, are not best placed to make the determination of whether a particular content is illegal, which requires careful balancing of competing interests and consideration of defences.[74]

The UN Special Rapporteur therefore recommended the following measures to address these problems.

– Censorship measures should never be delegated to private entities, and intermediaries should not be held liable for refusing to take action that infringes individuals' human rights.

- Any requests submitted to intermediaries to prevent access to certain content, or to disclose private information for strictly limited purposes such as the administration of criminal justice, should be done through an order issued by a court or other competent body which is independent of any political, commercial or other unwarranted influence.
- Corporations should act with due diligence to avoid infringing the rights of individuals.
- Corporations should establish clear and unambiguous terms of service in line with international human rights norms and principles and should continuously review the impact of their services and technologies on their users' right to freedom of expression, as well as on the potential pitfalls involved when they are misused.
- Intermediaries should only implement restrictions to fundamental rights after judicial intervention; and should be transparent to the user involved – and, where applicable, to the wider public - about measures taken;
- Intermediaries should provide forewarning to users before implementing restrictive measures; and should minimise the impact of restrictions strictly to the content involved.
- Intermediaries should disclose details about content removal requests and the accessibility of websites.
- There must be effective remedies for affected users, including the possibility of appeal through procedures provided by the intermediary and by a competent judicial authority.[75]

In their 2005 Joint Declaration, the four Rapporteurs on freedom of expression stressed that:

> No one should be liable for content on the internet of which they are not the author, unless they have either adopted that content as their own or refused to obey a court order to remove that content.[76]

The 2011 Joint Declaration reiterates that position and includes a non-monitoring recommendation:

> (a) No one who simply provides technical internet services such as providing access, or searching for, or transmission or caching of information, should be liable for content generated by others, which is disseminated using those services, as long as they do not specifically intervene in that content or refuse to obey a court order to remove that content, where they have the capacity to do so ('mere conduit principle').
>
> (b) Consideration should be given to insulating fully other intermediaries, including those mentioned in the preamble, from liability for content generated by others under the same conditions as in paragraph 2(a). At a minimum, intermediaries should not be required to monitor user-generated content and should not be subject to extrajudicial content takedown rules which fail to provide sufficient protection for freedom of expression (which is the case with many of the 'notice and takedown' rules currently being applied).[77]

At a regional level, the Council of Europe Declaration on Freedom of Communication[78], in line with the European Union Directive on Electronic Commerce (E-Commerce Directive),[79] generally exempts intermediaries from liability and calls upon member states "not to impose on service providers a general obligation to monitor content on the internet to which they give access, that they transmit or store, nor that of actively seeking facts or circumstances indicating illegal activity" since this might curb users' right to free speech. However, both the E-Commerce Directive and the Council of Europe Principles distinguish between the different functions and roles of access, service, hosting and content providers. Hence, the degree of liability depends on the online providers' ability to control content. Furthermore, the exclusion of a 'general' monitoring obligation does not preclude member states from imposing monitoring obligations on service providers in specific cases, such as criminal investigations. Only service providers that provide 'mere conduit' or access to communication are fully exempt from liability.[80] When service providers host third-party content they are liable only when they have 'actual knowledge' of the illegal nature of the content and do not remove it 'expeditiously' (notice and take-down principle) or if they make illegal content available (conditional 'safe harbour' principle).[81] Neither the E-commerce Directive nor the Council of Europe Principles stipulates safeguards against 'notice' abuse.

Linking liability

Liability for providing links to other websites on blogs, forums and chat rooms is another issue of concern. Several national courts have established liability for linking to illegal content or content deemed harmful, with most of the cases being concerned with links to websites and platforms containing copyrighted material.[82]

Linking liability is problematic for various reasons. As the material on the linked site can subsequently change, it makes people liable for content over which they have no control. Effectively, it assumes that people will constantly monitor all links that they previously made to ensure that they have not been changed. In addition, given the fact that people make links to materials on websites under various jurisdictions, it assumes that users will know the legislation of that jurisdiction in order to be able to determine the legality of the website they are linking to (a question many courts have proved unable to answer).

Enforcing linking liability in this way could result in people avoiding links for fear of liability, which would greatly hamper an essential part of the meaning and objective of the internet - to connect people to each other and to information.

In 2012, the European Court of Human Rights dealt with linking liability when it stated that:

> The internet being a public forum par excellence, the State has a narrow margin of appreciation with regard to information disseminated through this medium. This is even more the case as regards hyperlinks to web pages that are not under the de facto or de iure control of the hyperlinker. In this case, the narrow margin of appreciation of the State is determined by the principle that no liability may be imputed to the hyperlinker based on the illegal content of the hyperlinked web pages, except when the hyperlinker has de iure or de facto control of the hyperlinked web page or has endorsed the illegal content of the hyperlinked web page. Linking by itself cannot be understood as a tacit expression of approval, additional elements being necessary to evidence the deliberate mens rea of the hyperlinker."[83]

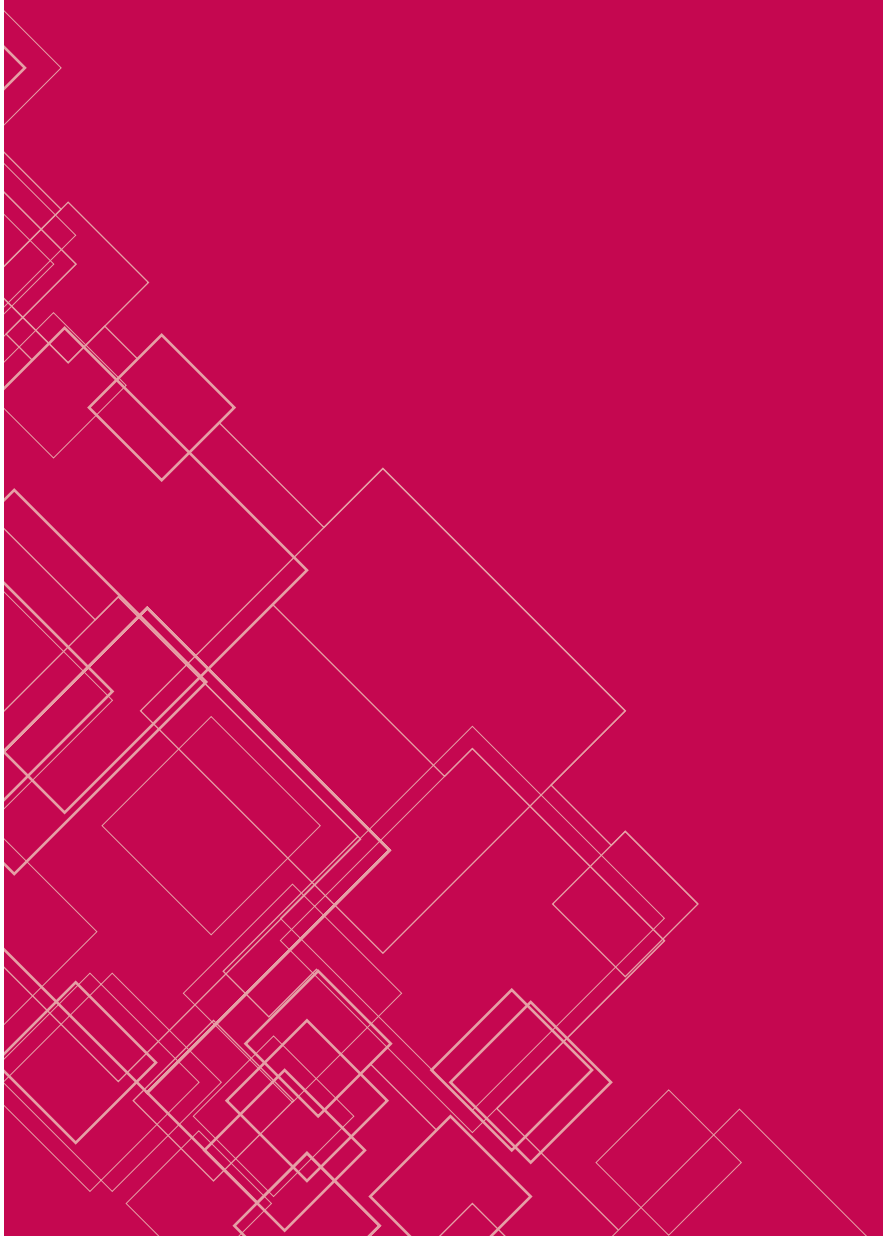
For comparative purposes, it is worth referring to a decision made by the Canadian Supreme Court in 2009 which stated that:

> Subjecting [hyperlinks] to the traditional publication rule would have the effect of seriously restricting the flow of information and, as a result, freedom of expression. The potential "chill" in how the internet functions could be devastating, since primary article authors would unlikely want to risk liability for linking to another article over whose changeable content they have no control. Given the core significance of the role of hyperlinking to the internet, we risk impairing its whole functioning. Strict application of the publication rule in these circumstances would be like trying to fit a square archaic peg into the hexagonal hole of modernity."[84]

The Canadian Supreme Court also upheld an earlier ruling of the British Columbia Court of Appeals in a case which stated that:

> A hyperlink is like a footnote or a reference to a website in printed material such as a newsletter. The purpose of a hyperlink is to direct the reader to additional material from a different source. The only difference is the ease with which a hyperlink allows the reader, with a simple click of the mouse, to instantly access the additional material.
>
> Although a hyperlink provides immediate access to material published on another website, this does not amount to republication of the content on the originating site. This is especially so as a reader may or may not follow the hyperlinks provided.
>
> Readers of a newsletter, whether in paper form or online, who read of a reference to a third party website, may go to that website. I conclude that that does not make the publisher of the web address a publisher of what readers find when they get there.[85]

Online content regulation



With the exponential growth of the internet and its ever-increasing number of users, governments have become progressively uneasy about the availability of a wide variety of online content which they cannot control. Indeed, the internet enables its users to gain access to information and ideas beyond the confines of the territory in which they reside. As different countries have different views on what content is illegal or may be deemed 'harmful' in line with their cultural, moral or religious traditions, online content regulation has become an important focus for governments across the globe.

By and large, states have been concerned with the availability of terrorist propaganda, racist content, hate speech, sexually explicit content including child pornography, blasphemous content, content critical of the government and its institutions and content unauthorised by intellectual property rights holders.

However, as the UN Special Rapporteur has rightly noted, these different types of content call for different legal and technological responses.[86] In 2011, the UN Special Rapporteur identified three different types of expression for the purposes of online regulation:

- Expression that constitutes an offence under international law which can be prosecuted criminally;
- Expression that is not criminally punishable but may justify a restriction and a civil suit; and
- Expression that does not give rise to criminal or civil sanctions, but still raises concerns in terms of tolerance, civility and respect for others.[87]

In particular, the Special Rapporteur clarified that the only exceptional types of expression that states are required to prohibit under international law are: (a) child pornography; (b) direct and public incitement to commit genocide; (c) hate speech; and (d) incitement to terrorism. He also clarified that even the legislation that criminalises these types of expression needs to be sufficiently precise, and that there must be adequate and effective safeguards against abuse or misuse, including oversight and review by an independent and impartial tribunal or regulatory body.[88]

In other words, these laws must also comply with the three-part test outlined above. For example, legislation prohibiting the dissemination of child pornography over the internet through the use of blocking and filtering technologies is not immune from those requirements.

Similarly, hate speech laws targeting online expression must be unambiguous, must pursue a legitimate purpose and must respect the principles of necessity and proportionality. In this regard, the Special Rapporteur has highlighted his concern that a large number of domestic provisions seeking to outlaw hate speech are unduly vague, in breach of international standards for the protection of freedom of expression. This includes expressions such as combating "incitement to religious unrest", "promoting division between religious believers and non-believers", "defamation of religion", "inciting to violation", "instigating hatred and disrespect against the ruling regime", "inciting subversion of state power" and "offences that damage public tranquillity."

The Special Rapporteur has also clarified which online restrictions are, in his view, impermissible under international law. In particular, he has called upon states to provide full details about the necessity and justification for blocking a particular website, stressing that the "determination of what content should be blocked should be undertaken by a competent judicial authority or a body which is independent of any political, commercial, or other unwarranted influences to ensure that blocking is not used as a means of censorship."[89]

Finally, the Special Rapporteur has highlighted that all other types of expression, such as defamatory comments, should not be criminalised. Instead, states should promote the use of additional speech to combat offensive speech. In this regard, it is worth mentioning that with new Web 2.0 types of applications, including the comment section on newspapers' websites, blogs, online chat rooms etc., it is now possible to respond to derogatory comments online almost immediately and at no cost. For this reason, the Special Rapporteur has remarked that the sanctions available for offline defamation and similar offences may well be unnecessary and disproportionate online.[90]

Cybercrime

Increasingly, countries are trying to regulate internet content through so-called "cybercrime legislation". At present, there is no universal definition of the term "cybercrime"[91], the term is usually used to describe any traditionally defined crime that is committed using a computer network or the internet. It typically covers a wide range of criminal offences from terrorist activities and espionage conducted with the help of the internet and illegal hacking into computer systems, to running boot nets[92] for the purpose of spreading spam emails and credit card fraud, phishing, theft and manipulation of data, and cyber-stalking, to name just a few.

Many of the recently adopted laws are, however, vague and overly broad and are therefore open to arbitrary and subjective interpretation, and threaten the protection of the right to freedom of expression. For example, in 2011, the UN Special Rapporteur on freedom of expression voiced the concern that:

> [L]egitimate online expression is being criminalized in contravention of States' international human rights obligations, whether it is through the application of existing criminal laws to online expression, or through the creation of new laws specifically designed to criminalize expression on the internet. Such laws are often justified on the basis of protecting an individual's reputation, national security or countering terrorism, but in practice are used to censor content that the Government and other powerful entities do not like or agree with.93

However, international standards on cyber-security do recognise the importance of balancing security imperatives with fundamental human rights, in particular the right to freedom of expression. The UN General Assembly Resolution on the Creation of a global culture of cyber security states that:

> Security should be implemented in a manner consistent with the values recognised by democratic societies, including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency.94

Likewise, the Council of Europe Convention on Cybercrime (2001) states that parties must be:

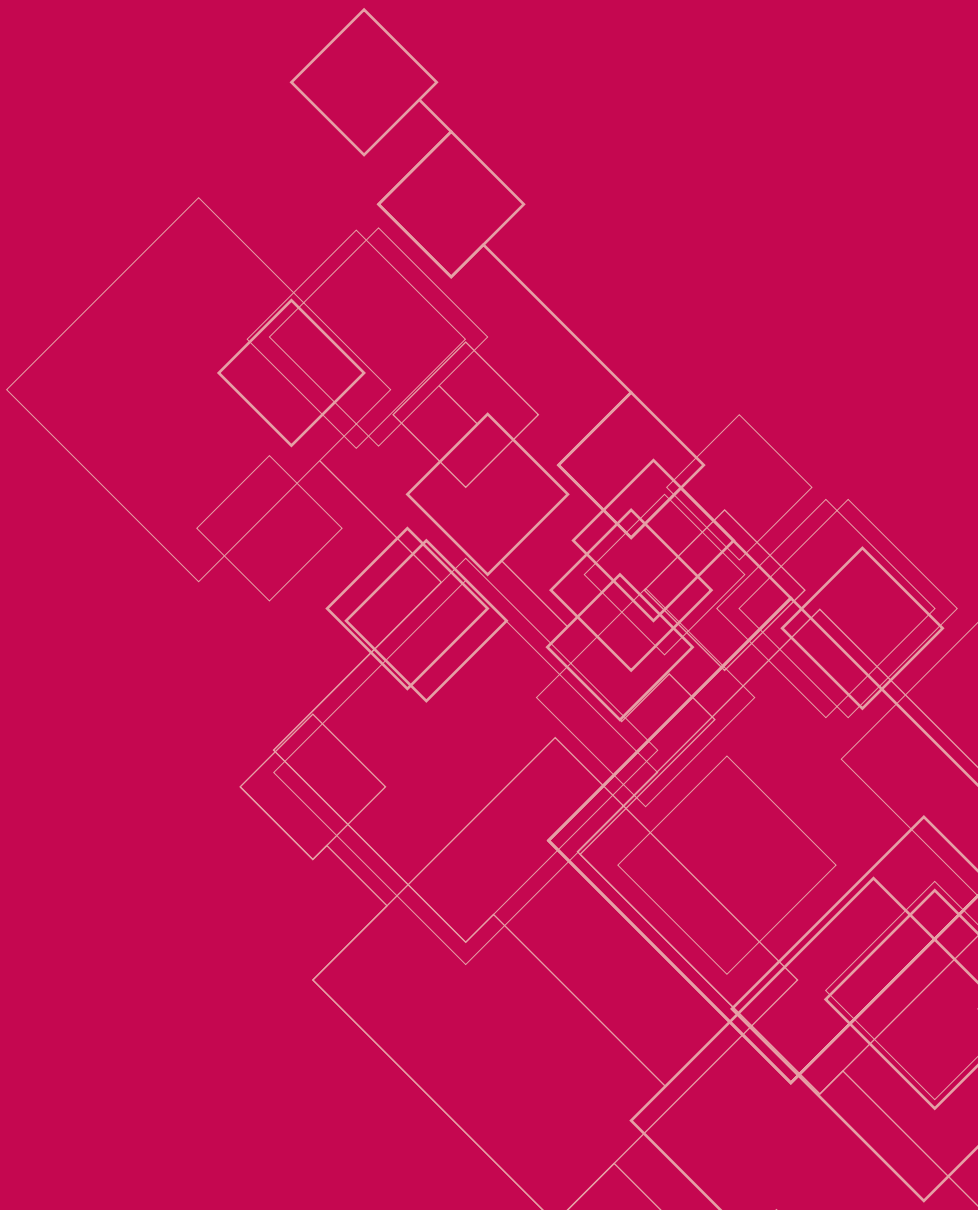
> [M]indful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights ... which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy.[95]

It is noteworthy that this convention contains no content-based restrictions other than those relating to child pornography. It should also be mentioned that the convention recognises the potential for domestic cybercrime laws to target political dissent and allows states to refuse assistance to other states if that request is perceived to relate to a politically motivated prosecution.[96]

Based on international standards, it can be concluded that legislation aimed at countering cybercrime has to be crafted in such a way that it is compatible with human rights law and international freedom of expression standards and must not be used to silence legitimate speech or to pursue critical citizens, human rights defenders, bloggers and journalists through electronic media. Cybercrime legislation should respect the proportionality principal that is fundamental to human rights protection and should meet the following criteria:

- Any legislation should provide for narrowly defined, clear and adequate definitions of key legal and technical terms covered by the offence.
- Legislation should require proof about the likelihood of harm arising from the criminal activity, including in relation to offences involving the obtaining or dissemination of classified information.
- Legislation should require the nature of the threat to national security resulting from any criminal activity to be identified.
- Legislation should provide for a public interest defence in relation to the obtaining and dissemination of information classified as secret.
- Legislation should refrain from imposing prison sentences for expression-related offences, except for those permitted by international legal standards and with adequate safeguards against abuse.[97]

The rights of citizen journalists and bloggers



The advent of the internet means that any individual can now publish his or her own opinions and ideas on a blog or social media network. This raises the question of how journalism should be defined and what constitutes 'media' in the digital age. Equally, the question arises as to whether and, if so, how 'citizen journalists' and 'bloggers' should be regulated.

In short, there is currently no set definition of journalism or what constitutes 'media' in the digital age at an international level. Nonetheless, the UN Human Rights Committee and the Council of Europe have provided tentative responses, which are set out below. As far as the question of regulation is concerned, it is clear that international law does not require bloggers and citizen journalists to register, let alone register under their real name. However, there are no clear standards on the following two questions: first, whether, and if so, what professional standards should be applied to citizen journalists and bloggers; and secondly, whether citizen journalists and bloggers should be able to make use of a journalist's right to protect his or her sources.

Definition of journalism and new media

In its General Comment No. 34, the UN Human Rights Committee defined journalism as follows:

> 44. Journalism is a function shared by a wide range of actors, including professional full-time reporters and analysts, as well as bloggers and others who engage in forms of self-publication in print, on the internet or elsewhere, and general State systems of registration or licensing of journalists are incompatible with paragraph 3. Limited accreditation schemes are permissible only where necessary to provide journalists with privileged access to certain places and/or events. Such schemes should be applied in a manner that is non-discriminatory and compatible with article 19 and other provisions of the Covenant, based on objective criteria and taking into account that journalism is a function shared by a wide range of actors.

The UN Human Rights Committee has therefore taken a functional approach to the definition of journalism. In other words, journalism is an activity, which consists of the collection and dissemination of information to the public via any means of mass communication.

On a regional level, the Council of Europe (COE) has taken a similar approach in its recent Recommendation CM/Rec (2011)7 on a new notion of 'media'. In that recommendation, the Committee of Ministers called on member states to:[98]

– [A]dopt a new, broad notion of media which encompasses all actors involved in the production and dissemination, to potentially large numbers of people, of content (for example information, analysis, comment, opinion, education, culture, art and entertainment in text, audio, visual, audiovisual or other form) and applications which are designed to facilitate interactive mass communication (for example social networks) or other content-based large-scale interactive experiences (for example online games), while retaining (in all these cases) editorial control or oversight of the contents; [emphasis added]

– [Review] regulatory needs in respect of all actors delivering services or products in the media ecosystem so as to guarantee people's right to seek, receive and impart information in accordance with Article 10 of the European Convention on Human Rights, and to extend to those actors relevant safeguards against interference that might otherwise have an adverse effect on Article 10 rights, including as regards situations which risk leading to undue self-restraint or self-censorship; [emphasis added]

The Committee of Ministers further offered a number of criteria to be taken into account when determining whether a particular activity or actor should be considered as media, namely: (i) intent to act as media; (ii) purpose and underlying objectives of media; (iii) editorial control; (iv) professional standards; (v) outreach and dissemination; and (vi) public expectation.

In addition, the Committee provided a set of indicators for determining whether a particular criterion is fulfilled. For example, a particular organisation or individual engaged in the dissemination of information will fully meet the public expectation criterion if the information is available, reliable, provides content that is diverse and respects the value of pluralism, respects professional and ethical standards, and is accountable and transparent. At the same time, the Council of Ministers highlighted that each of the criteria should be applied flexibly.

Interestingly, the Committee said that bloggers should only be considered to be media if they meet certain professional standards to a sufficient degree. It is helpful to note, however, that in the United Kingdom, the Code of Practice applies to citizen journalists only to the extent that they submit material to newspapers and magazines that subscribe to the Code.99 The Press and Complaints Commission (PCC) has thus clarified that "Editors and publishers (who take the ultimate responsibility under the self regulatory system) are required to take care to ensure that the Code is observed not only by editorial staff, but also by external contributors, including non-journalists". This strongly implies that unless bloggers submit materials to newspapers, they should not be made subject to the same onerous duties and responsibilities as professional journalists.

Regulation of bloggers and citizen journalists

Registration

The UN Human Rights Committee's definition of journalism (outlined above) clearly shows that, like professional journalists, bloggers should not be subject to registration or licensing requirements. Similarly, they should be accredited only where this is necessary to get privileged access to certain places and/or events.

Limited editorial control

In its CM/Rec (2011)7 on a new notion of 'media' mentioned above, the Committee of Ministers of the Council of Europe recognised that different levels of editorial control call for different levels of editorial responsibility. In particular, it said that:

> Different levels of editorial control or editorial modalities (for example ex ante as compared with ex post moderation) call for differentiated responses and will almost certainly permit best to graduate the response.[100]

This suggests that any legal framework affecting bloggers and citizen journalists should recognise that they have more limited duties and responsibilities when exercising their freedom of expression than professional journalists because they do not have the same resources and technical means as newspapers.

Civil and criminal liability

The law does not generally make any distinctions between journalists and the rest of the population for the purposes of civil or criminal liability. Accordingly, bloggers and citizen journalists are not immune to the application of laws such as defamation laws. Nonetheless, the question arises as to whether bloggers and citizens should benefit from the same legal protections as journalists when they undertake the activity of journalism.

Legal protection

There are no set international legal standards concerning the legal protection which should be afforded to citizen journalists and bloggers at present. However, in the same way that bloggers have a duty, like any other citizen, to obey the law, they can also make use of the defences available to citizens under the law.

The question of whether bloggers and citizen journalists can avail themselves of legal principles governing the protection of sources is more controversial. In Recommendation CM/Rec (2011)7 cited above, the Committee of Ministers said that:

> [T]he protection of sources should extend to the identity of users who make content of public interest available on collective online shared spaces which are designed to facilitate interactive mass communication (or mass communication in aggregate); this includes content-sharing platforms and social networking services. Arrangements may be needed to authorise the use of pseudonyms (for example in social networks) in cases where disclosure of identity might attract retaliation (for example as a consequence of political or human rights activism).

However, it is not clear from the recommendation whether a blogger or citizen journalist could avail himself or herself of the protection of sources in relation to information received from internet users or others. Nonetheless, the Committee of Ministers has recommended that some form of support and protection should be provided to those media actors, e.g. bloggers, who do not fully qualify as media under a number of criteria set forth by the Committee but who do 'participate in the media ecosystem'.[101]

Access to information and ICTs

There is a global trend towards states, intergovernmental organisations, civil society and other people recognising the right to information. There is a growing body of authoritative statements supporting the right to information made in the context of official human rights mechanisms. Numerous laws giving effect to this right have, in the last few years, been adopted in all regions of the world. Many intergovernmental organisations have put in place information disclosure systems which are reviewed and updated on a regular basis.

From the ICT perspective, there are two issues that deserve particular attention: e-government and open data.

E-governance and e-government

The terms e-governance and e-government are sometimes used interchangeably.

UNESCO defines e-governance as:

> The public sector's use of information and communication technologies with the aim of improving information and service delivery, encouraging citizen participation in the decision-making process and making government more accountable, transparent and effective.[102]

E-government is typically defined as the use of information and communications technologies by governments to enhance the range and quality of information and services provided to citizens, businesses, academia, the media and public institutions in an efficient, less bureaucratic, cost-effective manner. A UN study on the state of e-government defines e-government as "utilizing the internet and the world-wide-web for delivering government information and services to citizens".[103]

The goal of e-government is not merely for government agencies to have web presences or to computerise or digitise governmental records but also to optimise government services and make them more speedy, accessible and transparent through information communications technologies. E-government transforms the way governments interact with citizens, business and other governments. Examples of e-government include e-tax, e-health and e-transportation.

Any meaningful e-government approach needs to start by ensuring a full rollout of the basic internet infrastructure that provides fast internet connection to all citizens, and non-discriminatory access to e-services. Governments need also to invest in internet and digital literacy in order to strengthen citizens' ability to make use of e-services.

Governments must also ensure that information and services provided through an e-government approach are reliable and that information being provided by users is strongly protected both technologically and legally against surveillance and misuse. E-governments need to enact strong privacy legislation that bans linking and combining personal data submitted to different and non-related e-services, making it possible to create profiles of users ('the transparent citizen').

The provision of e-services by governments also needs to follow clear rules and be transparent in terms of knowing which public body is offering which services under which conditions and with which safeguards. For example, governments are turning more and more to social networking sites to reach out to citizens. Wherever governments leave their official e-presence (or website) to enter public online spheres like social networking platforms or to engage in online discussions with their constituency, this should be done in a clear, non-misleading way and include various (offline) contact details for the responsible public officials in charge of that service.

Finally, governments should install independent oversight and complaints mechanisms for all e-government services in order to ensure that these services function properly; redress mechanisms for citizens whose rights might have been violated by an e-service; and whistleblower hotlines to which wrongdoings and corruption can be reported anonymously and safely.

Open data

Open data characterises the free availability of public data or data collected, either by public, private or non-governmental organisations, on behalf of the public in the interest of that society. As such, open data has to be regarded as a common resource. Open data might be statistical data, geographical information and maps, traffic and spatial data, scientific publications and medical research made possible with public funds, non-personal data collected by law enforcement, courts and public administration.

Open data is an essential precondition in the digital age for more democratic participation, transparency, open and efficient government, but also for creativity, innovation and economic growth.

Open data is reliant on effective freedom of information legislation. Under international law, governments must show that any restrictions on access to information are prescribed by law, necessary in a democratic society and pursue a legitimate aim. Limits on access to information and restrictions to open data should only apply if both governments and private bodies can demonstrate that making such data available would cause a specific and articulated harm to the fundamental rights of others or to society. The fear of economic disadvantage does not constitute this type of harm.

Governments and private entities have been slow to open the databases which were created by collecting data with public funds for the public. Many governments withhold such public data and often governmental work is carried out by private contractors who then retain the data they collected on behalf of the government or make it available subject to hefty fees. Only a few governments follow open data policies.[104]

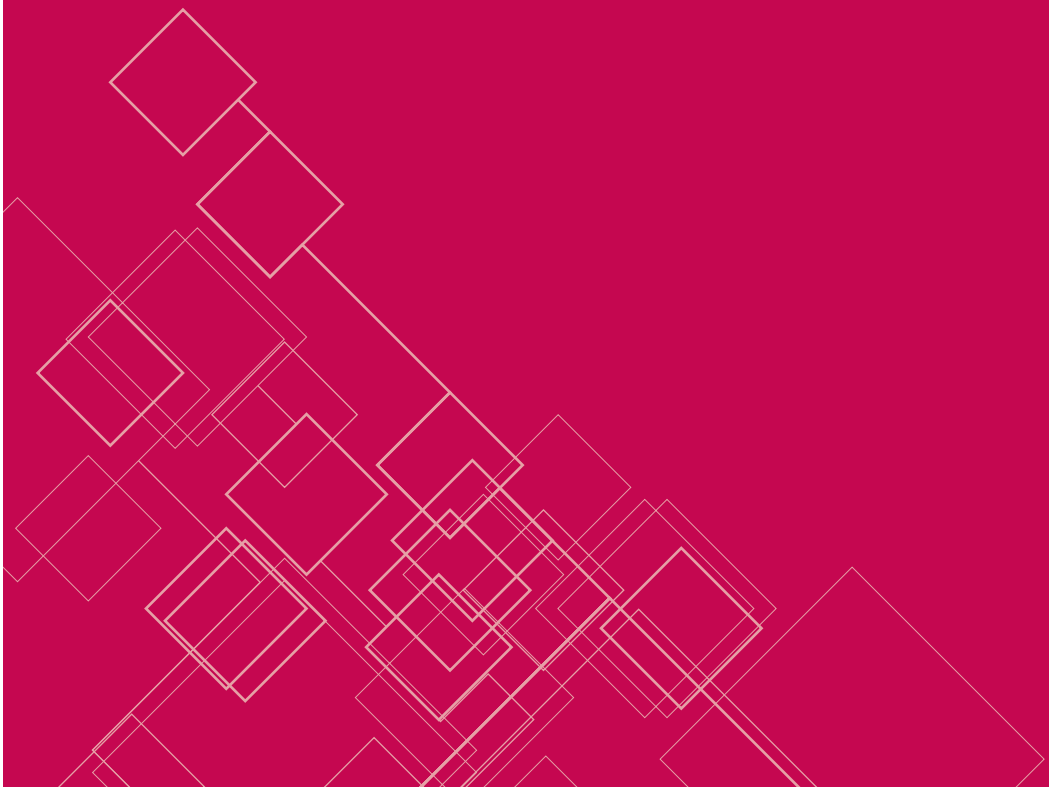
At international level, the Berlin Declaration on Open Access to Knowledge in the Sciences and Humanities[105] was adopted in 2003 by almost 500 universities, research and scientific centres, and libraries worldwide. Its objective is to provide free and global access to the world's scientific and cultural heritage. The declaration defines two conditions for meaningful open access:

> The author(s) and right holder(s) of such contributions grant(s) to all users a free, irrevocable, worldwide, right of access to, and a license to copy, use, distribute, transmit and display the work publicly and to make and distribute derivative works, in any digital medium for any responsible purpose, subject to proper attribution of authorship (community standards, will continue to provide the mechanism for enforcement of proper attribution and responsible use of the published work, as they do now), as well as the right to make small numbers of printed copies for their personal use.
>
> A complete version of the work and all supplemental materials, including a copy of the permission as stated above, in an appropriate standard electronic format is deposited (and thus published) in at least one online repository using suitable technical standards (such as the Open Archive definitions) that is supported and maintained by an academic institution, scholarly society, government agency, or other well established organization that seeks to enable open access, unrestricted distribution, interoperability, and long-term archiving.[106]

Open data requires a commitment to make information and data resources accessible to all without discrimination and to provide open data license agreements. Given the sheer amount of potential open data, information classified as open data should also be processed in such a way that makes it possible to navigate easily through databases and filters using keywords in order to be able to find the required information in a short time.

An important aspect of every open data policy, from a human rights point of view, is to ensure that there is a firm distinction between non-personal data that should be open and freely available and personal data that enjoys protection under international human rights standards.

Regulatory framework of the internet



Internet governance

The internet evolved outside any legal and regulatory frameworks and without guidance or supervision by intergovernmental organisations, such as the International Telecommunications Union (ITU). From its beginning it was a global endeavour and, as such, was not subject to the jurisdiction of a particular state and government. It developed through what we call today "multi-stakeholder" processes that included state and non-state actors and was mainly based on self-regulation by its users and interoperable codes agreed upon by those providing its infrastructure and services.

Although, the term "internet governance" is not a clearly specified term and covers a range of governance issues, the key aspect concerns the question of what groups, if any, should have oversight of the different technical, economic, regulatory and legal aspects that touch upon the decentralised framework in which the internet is embedded.

Despite the non-hierarchical set-up of the internet, there are features that follow strict hierarchical rules. This is the case with the Domain Name System (DNS), consisting of 13 root servers, which is managed by the US-registered internet Corporation for Assigned Names and Numbers (ICANN). The DNS defines how web addresses and generic top-level domains (such as .com and .org) and country-code top-level domain names (such as .uk and .za) are translated into internet Protocol (IP) addresses. ICANN is accountable to the US Department of Commerce based on a Memorandum of Understanding[107] and was registered under Californian law.[108] Changes to the specifications of the root servers are only possible after approval by the Department of Commerce. The particular administrative structure of ICANN has led to criticism by many states who have argued that changes to their country-code top-level domains would only be possible with the consent of the US Government. These countries would prefer to internationalise this technical aspect of internet governance and place it under an intergovernmental umbrella and international law.[109]

The topic of how and by whom the internet should be governed was the subject of the first World Summit on the Information Society (WSIS) under the umbrella of the UN in Geneva in December 2003 and attended by 175 governments.[110] At this forum, the term "Internet Governance" was created in order to give the complexity of the issue a name.

The summit in Geneva did not yield the expected results in terms of internet Governance; however, it did produce the Geneva Declaration of Principles[111] which stressed that:

> Communication is a fundamental social process, a basic human need and the foundation of all social organization. It is central to the Information Society. Everyone, everywhere should have the opportunity to participate and no one should be excluded room the benefits the Information Society offers.[112]

The principles also called upon all actors to:

> [T]ake appropriate actions and preventive measures, as determined by law, against abusive uses of ICTs, such as illegal and other acts motivated by racism, racial discrimination, xenophobia, and related in tolerance, hatred, violence, all forms of child abuse, including paedophilia and child pornography, and trafficking in, and exploitation of, human beings.[113]

The first WSIS was followed by a Working Group on internet Governance (WGIG) tasked to elaborate a clear definition of the term "Internet Governance," to discuss the possibility of international oversight over critical internet resources and to specify the questions and different problems related to it, as well as to draft recommendations for political decision makers. The WGIG confirmed that internet governance issues include important legal aspects, including privacy rights, intellectual property rights, cybercrime, and data protection and that they should discuss mechanisms for addressing issues such as self-regulation and jurisdiction.

In the run-up to the second WSIS held in Tunis in November 2005 and attended by around 170 governments, several states favoured the internationalisation of ICANN as well as, more generally, internet governance within a UN framework.[114] The European Union suggested the "establishment of an arbitration and dispute resolution mechanism based on international law in case of disputes" for all "naming, numbering and addressing-related matters."[115]

The WSIS in Tunis did not yield any results or agreement as to how to govern the internet in the future but, similar to the first WSIS of 2003, its concluding documents, the Tunis Commitments and the Tunis Agenda for the Information Society, recognised that "freedom of expression and the free flow of information, ideas, and knowledge, are essential for the Information Society and beneficial to development."[116] The Tunis Agenda also provided a "working definition of internet governance":

> [T]he 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.[117]

In order to avoid the Summit failing, it was agreed to add a third forum to the WSIS and the WGIG, the internet Governance Forum (IGF). According to the Tunis Agenda, the IGF should be multilateral, multi-stakeholder, democratic and transparent. Among other points, it is mandated to:

- Public policy issues relating to key elements of internet governance in order to foster the sustainability, robustness, security, stability and development of the internet.
- Interface with appropriate intergovernmental organisations and other institutions on matters under their purview.
- Promote and assess, on an ongoing basis, the embodiment of WSIS principles in internet governance processes.
- Help to find solutions to issues arising from the use and misuse of the internet which are of particular concern to everyday users.[118]

The IGF was first held in 2006 in Athens and is now being organised annually. It has no decision-making powers and can only issue non-binding recommendations.

While the annually held WSISs and IGFs keep discussing whether the internet or aspects of it would benefit or suffer from an institutionalised and legally framed governance keeping it as a free and open platform, one of its backbones, the DNS, continues to be managed by ICANN which still remains accountable to the U.S. Department of Commerce.

Regional initiatives

In 2011, the Council of Europe adopted Ten internet Governance Principles.[119] The principles, inter alia, endorse the universality, openness, and integrity of the internet, the multi-stakeholder approach to internet governance, and the decentralised management and interoperability of the internet. They stipulate that:

> 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 up hold 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.

It is most noteworthy that, along with public actors, private actors are called upon to respect human rights and fundamental freedoms when developing, offering and operating their services and applications.

Jurisdiction

The global nature of the internet no longer respects strict boundaries and the control of individual states. Some governments fear that the internet is undermining their judicial sovereignty as extraterritoriality is a major problem whenever culturally, morally or politically sensitive content is at question.

Development of international standards and jurisprudence has been slow. However, the following initiatives and standards should be mentioned:

– In the 2003 Amsterdam Recommendations, the OSCE Representative on Freedom of the Media demanded that "illegal content must be prosecuted in the country of its origin."[120] 'Origin' remains a vague term, as the Representative did not specify whether the content must have been produced or uploaded in, aimed at the audience of a particular country, or written in the language(s) or by a citizen or resident of that country.

– The 2005 Joint Declaration of special mandates on freedom of expression specified the question of 'origin' by stating that "jurisdiction in legal cases relating to internet content should be restricted to States in which the author is established or to which the content is specifically directed; jurisdiction should not be established simply because the content has been downloaded in a certain State."[121] In their 2010 Joint Declaration, special rapporteurs expressed concern about "jurisdictional rules which allow cases, particularly defamation cases, to be pursued anywhere, leading to a lowest common denominator approach"[122], but did not offer further jurisdictional guidelines.

– The 2011 Joint Declaration of special mandates stressed that "jurisdiction in legal cases relating to internet content should be restricted to States to which those cases have a real and substantial connection, normally because the author is established there, the content is uploaded there and/or the content is specifically directed at that State. Private parties should only be able to bring a case in a given jurisdiction where they can establish that they have suffered substantial harm in that jurisdiction."[123] It should, however, be mentioned that the so-called 'upload-rule' (whereby liability for content is attached to the jurisdiction where the material has been uploaded) and the 'download-rule' (which makes content subject to all the jurisdictions where information has been downloaded) are – on their own and outside of a wider context – flawed and permissive as they encourage 'forum shopping' and risk playing off one jurisdiction against the other. The 'download-rule' would also require users, authors, publishers and hosting companies to be subject at all times to the legislation of all the jurisdictions where their content might be read and accessed.

End notes

[1] See, for example, OSCE, Freedom of Expression and the internet, 2010; available at http://www.osce.org/fom/80723. The 2011 Report of the UN Special Rapporteur on Freedom of Expression, A/66/290, 10 August 2011; available at http://www.ohchr.org/Documents/Issues/Opinion/A.66.290.pdf

[2] Universal Declaration of Human Rights, UN General Assembly Resolution 217A (III), 10 December 1948.

[3] See, Filartiga v. Pena-Irala, 630 F. 2d 876 (1980) (US Circuit Court of Appeals, 2nd circuit).

[4] International Covenant on Civil and Political Rights, UN General Assembly Resolution 2200A (XXI) of 16 December 1966, entered into force 23 March 1976.

[5] General Comment No 34, CCPR/C/GC/3.

[6] Ibid., para. 12.

[7] Ibid., para. 17.

[8] Ibid., para. 39.

[9] UN Human Rights Council Resolution A/HRC/20/L.13, adopted 29 June 2012.

[10] The 2011 Report of the UN Special Rapporteur, op.cit, para 16.

[11] Joint Declaration of four special mandates on Freedom of Expression and the internet, June 2011, available at http://www.osce.org/fom/78309. Moreover, two other joint declarations of special mandates dealt with internet freedoms: the 2005 Joint Declaration on internet and Anti-Terrorism and the 2010 Joint Declaration Ten Key Challenges. All joint declarations of special mandates on freedom of expression are available at http://www.osce.org/fom/66176.

[12] Ibid., the 2011 Joint Declaration on Freedom of Expression and the Internet.

[13] Ibid.

[14] See, HR Committee, Velichkin v. Belarus, Communication No. 1022/2001, U.N. Doc. CCPR/C/85/D/1022/2001 (2005).

[15] See, HR Committee Leonardus J.M. de Groot v. The Netherlands, No. 578/1994, U.N. Doc. CCPR/C/54/D/578/1994 (1995).

[16] HR Committee, Concluding observations on the Syrian Arab Republic, CCPR/CO/84/SYR.

[17] Ibid.

[18] The 2011 Report of the UN Special Rapporteur on Freedom of Expression, op.cit.

[19] Adopted 27 June 1981, OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), entered into force on 21 October 1986.

[20] Adopted at the 32nd Session of the African Commission on Human and Peoples' Rights, 17-23 October 2002/.

[21] American Declaration of the Rights and Duties of Man, OEA/Ser.L./V.II.23, doc. 21, rev. 6 (1948).

[22] Adopted at the Inter-American Specialized Conference on Human Rights, 22 November 1969, OAS Treaty Series No.36; 114 UNTS 123; 9 ILM 99 (1969), entry into force 18 July 1978.

[23] Adopted by the Inter-American Commission on Human Rights at its 108th Regular Session, 19 October 2000, available at http://www.iachr.org/declaration.htm.

[24] Available at http://www.asean.org/news/asean-statement-co.mmuniques/item/asean-human-rights-declaration.

[25] Adopted on 22 May 2004, entered into force on 15 March 2008.

[26] Adopted on 4 November 1950, entry into force 3 September 1953.

[27] Charter of Fundamental Rights of the European Union, 2000/C 364/01, adopted 7 December 2000, entry into force 1 December 2009; available at http://www.europarl.europa.eu/charter/pdf/text_en.pdf. Article 11 reads: "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. The freedom and pluralism of the media shall be respected."

[28] Recommendation CM/Rec(2011)7.

[29] Recommendation CM/Rec(2011)8.

[30] For example, in 2005 - 2010, the European Court decided on only ten cases related to freedom of expression and ICTs (Internet, email, and electronic data); and in 2011-July 2013, it decided, however, on eight cases. See overview at: http://www.echr.coe.int/Documents/FS_New_technologies_ENG.pdf.

[31] In November 2011 the European Court of Justice (ECJ) issued two important decisions. In Scarlet Extended SA vs SABAM, C-70/10, the ECJ delivered a landmark case for the protection of free speech in the fight against online "piracy" in which it decided that measures ordering ISPs to install filtering and blocking systems to prevent illegal file-sharing on peer-to-peer networks was in breach with fundamental rights, particularly the right to privacy and the freedom of information; available at http://curia.europa.eu/juris/liste.jsf?language=en&num=C-70/10. In SABAM vs Netlog, Case C360/10, in February 2012, the ECJ confirmed that general monitoring and filtering systems

installed for the prevention of intellectual property infringements are disproportionate. It ruled that like ISPs, social networks cannot be ordered o monitor and filter their users' communications to prevent copyright infringements; available at http://curia.europa.eu/juris/document/document.jsf?docid=119512&doclang=EN.

[32] See, for example, testimony of the OSCE Special representative on freedom of the media to the U.S. Helsinki Commission in July 2011; available at http://www.osce.org/fom/81006.

[33] Declaration of Principles, Building the Information Society: a global challenge in the new Millennium, WSIS-03/GENEVA/DOC/4-E, 12 December 2003, available from: http://www.itu.int/wsis/docs/geneva/official/dop.html.

[34] General Comment No. 34, para 15.

[35] The 2011 Report of the UN Special Rapporteur, op.cit., para 79.

[36] Ibid., para 3.

[37] Ibid. para 85.

[38] The 2011 Joint Declaration, op. cit., para 6 e).

[39] Office of the OSCE Representative on Freedom of the Media, Freedom of Expression on the internet: A Study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the internet in OSCE participating States, p. 14.

[40] Article 5A para 2 of the Greek Constitution stipulates that "all persons have the right to participate in the Information Society. Facilitation of access to electronically transmitted information, as well as of the production, exchange and diffusion thereof, constitutes an obligation of the State, always in observance of the guarantees of articles 9, 9A and 19."

[41] The 2000 Telecommunications Act of Estonia, Article 5 para 1 states that "all customers who wish to have access to the public telephone network shall have such access for a uniform and reasonable consideration;" this shall include "Internet service which is universally available to all subscribers regardless of their geographical location, at a uniform price." Further, the 2000 Public Information Act, Article 33, guarantees everyone "the opportunity to have free access to public information through the internet in public libraries."

[42] In Decision 2009-580 DC of 10 June 2009, the French Constitutional Council, ruling on the constitutionality of so-called Hadopi-I Law, declared access to online services to be a basic human right.

[43] The Amendment No. 331/2009 of the Communications Market Act of Finland, Law No. 393/2003, obliges telecommunication companies to provide each Finish citizen with an internet connection of at least one megabit per second, the aim being an internet speed of 100 megabit/second by 2015.

[44] The Law No. 2/11 of March 2011, Sustainable Economy --in Article 52 added broadband access to its universal service, and stipulated that broadband connection at a speed of 1Mbit per second is to be provided through any technology. It also states that the conditions of broadband access to the public are to be established by royal decree within four months from entry into force of the Law.

[45] In Court Decision No. 09-013141-0007-CO of 30 July 2010, the Supreme Court of Costa Rica ruled that "access to [information technology and communication] technologies becomes a basic tool to facilitate the exercise of fundamental rights and democratic participation... This includes the fundamental right of access to these technologies, in particular, the right of access to the internet or World Wide Web."

[46] See, for example, Body of European Regulators for Electronic Communications, A view of traffic management and other practices resulting in restrictions to the open internet in Europe, 29 May 2012.

[47] Ibid.

[48] The 2011 Joint Declaration, op.cit., Article 5.

[49] Adopted at 3134th Transport, Telecommunications and Energy Council Meeting, Brussels, 13 December 2011; available at http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/trans/126890.pdf.

[50] These are European Parliament resolution on the open internet and net neutrality in Europe, adopted 17 November 2011, P7_TA(2011)0511.

[51] European Parliament resolution on completing the Digital Single Market, adopted 11 December 2012, 2012/2030(INI).

[52] European Parliament resolution on a Digital Freedom Strategy in EU Foreign Policy, adopted 11 December 2012, 2012/2094(INI).

[53] Chile was the first country to set forth net neutrality requirements in amendments to its telecommunications law that came into force in May 2011. The ISPS are not permitted to slow down, block, restrict or discriminate against content, applications or services; see http://www.neutralidadsi.org/2010/07/13/camara-de-diputados-aprueba-el-proyecto-de-ley-de-neutralidad-en-la-red/.

[54] The amendments to the Telecommunications Law of 8 May 2012, prevent telecom providers from blocking or throttling services such as Skype or WhatsApp, an internet SMS [Short Message Service and from making prices for their internet services dependent on the services used by the subscriber. While traffic may be throttled in order to prevent congestion or protect the network (provided that the ISPs "treat traffic of the same type equally"), it may not be blocked except when necessary "to protect the integrity and security of the network or users' terminals."

[55] Article 203 The Economic Communications Law of 20 December 2012 includes net neutrality, confirming the open and neutral character of the internet and obliging ISPs and network operators "to preserve the open and neutral character of the internet such that they do not hinder, withhold or slow down internet traffic at the level of individual services or applications, or take measures to degrade these services or applications." Exception include the prevention of network congestion, the preservation of the integrity and security of the network, measures to restrict unsolicited communications as provided by law and. a court decisions. The Law stipulates that exceptions must "be proportionate, non-discriminatory, subject to a time-limit and carried out to the extent necessary to achieve their objectives.".

[56] On 21 December 2010, the US Federal Communications Commission (FCC) published 'Formal Complaint Procedures, Preserving the Open internet and Broadband Industry Practices' (FCC 10-201), aimed at ensuring net neutrality. The rules espouse three basic principles: all ISPs must be transparent in their network management practices; ISPs are prohibited from blocking lawful sites and services; and fixed broadband providers cannot unreasonably discriminate against lawful network traffic.

[57] The first law was introduced in France in 2009, Act furthering the diffusion and protection of creation on the internet (HADOPI-I Law). However, the French Constitutional Council, in Decision 2009-580 DC of 10 June 2009, declared the law in violation of the Declaration of the Rights of Man and of the Citizens, and decided only a court of law or a judge could issue a decision to cut access to the web. Subsequent HADOPI-II included the requirement of judicial review before the suspension of a user's internet access; however, the disconnection of up to one year was kept. Finally, on 9 July 2013, the Government issued a degree announcing that it will no longer allow suspension of internet access as a punitive measure, see http://www.culturecommunication.gouv.fr/Espace-Presse/Communiques/Publication-du-decret-supprimant-la-peine-complementaire-de-la-suspension-d-acces-a-Internet. However, judges will be able to continue imposing fines of up to 1,500 EUR for repeated infringements. Similar legislation was passed in the UK with the Digital Economy Act 2010 under sections 3-16. Due to legal challenges by British ISPs, that argued that the Act was incompatible with EU privacy provisions and put an unfair financial burden on ISPs, entry into force of certain sections of Act have been delayed. Although, two provisions allowing courts to block access to particular websites were dropped after heavy criticism, the Act allows Ofcom to apply a graduated response in cases of copyright infringement, including applying a technical measure that (a) limits the speed or other capacity of the service provided to a subscriber; (b) prevents a subscriber from using the service to gain access to particular material, or limits such use; (c) suspends the service provided to a subscriber; or (d) limits the service provided to a subscriber in another way.

[58] The 2011 Report of the Special Rapporteur, op.cit., paras 78 and 79.

[59] The 2011 Joint Declaration, op.cit., Article 6c).

[60] See SABAM vs Netlog, op.cit.; and Scarlet Extended SA vs. SABAM, op.cit.

[61] For example, in Turkey, the majority of content is not blocked based on court rulings, but based on decisions taken by an administrative body.

[62] See, for example, Office of the OSCE Representative on Freedom of the Media, Freedom of Expression on the internet – A study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the internet in OSCE participating States, 2012, p. 204ff.

[63] The 2011 Joint Declaration, op. cit. . Article 3.

[64] See Ahmet Yıldırım v. Turkey, Application no. 3111/10, decision of 18 December 2012. The case concerned the decision to block access to the Google Sites internet domain, which, among other, hosted the applicant's site and a website of a user facing criminal charges for insulting the memory of Atatürk. The Court found out that the measure was not prescribed by law as it was not reasonably foreseeable in accordance with the rule of law. Moreover, the decision to block all of Google Sites stemmed from a request by an administrative body to extend the initially limited scope of the judicial blocking order (limited to the specific site) to the entire domain. The Court further found that the Turkish Court had failed to apply the necessity test when deciding on the blocking.

[65] The 2011 report of the UN Special Rapporteur, op.cit.

[66] Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines, adopted by the Committee of Ministers, 4 April 2012.

[67] Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services, adopted by the Committee of Ministers on 4 April 2012.

[68] For example, wired.com reported that between mid-2010 and mid-2013, the US law enforcement authorities, using civil forfeiture provisions, have seized over 1,700 domain names of websites and blogs that allegedly breached intellectual property rights provision (under 'Operation in Our Sites'. Programme). Many of these domains were operated legally from outside the United States; see http://www.wired.com/threatlevel/2013/06/domains-seized.

[69] ACLU, ICE Doman Name Seizures Threaten Due Process and 1st Amendment Rights, 20 June 2012; available at http://www.aclu.org/blog/free-speech-national-security-technology-and-liberty/ice-domain-name-seizures-threaten-due.

[70] States pursue different approaches in regards to intermediary liability, from expansive protections against intermediary liability, to conditional liability (notice and take-down approach), and blanket or strict liability for intermediaries. For more information, see ARTICLE 19, internet Intermediaries: Dilemma of Liability, August 2013.

[71] For example, Freedom House notes that, of the 47 countries it recently examined, 20 had experienced negative developments since 2011. Even in those countries with notable improvements, the general trend was towards more restrictions on internet freedom See Freedom House, Freedom on the Net 2012, p. 1, available at http://www.freedomhouse.org/sites/default/files/resources/FOTN%202012%20Overview%20Essay.pdf.

[72] This is, for example, a case of Russia; see http://www.nytimes.com/2013/04/01/technology/russia-begins-selectively-blocking-internet-content.html?_r=0.

[73] See, Joe McNamee, internet intermediaries: the new cyber police?, 2011, available at http://www.giswatch.org/en/freedom-association/internet-intermediaries-new-cyberpolice.

[74] UN Human Rights Council Document A/HRC/17/27 of 16 May 2011, available from: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

[75] The 2011 Report of the UN Special Rapporteur, op.cit.

[76] International Mechanisms for Promoting Freedom of Expression, Joint Declaration on internet and Anti-Terrorism, 21 December 2005.

[77] The 2011 Joint Declaration, op.cit., Article 2.

[78] Council of Europe, Committee of Ministers, Declaration on freedom of communication on the internet, adopted 28 May 2003.

[79] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).

[80] Ibid. and Declaration on Freedom of communication on the internet, op.cit.

[81] Declaration on Freedom of communication on the internet, Ibid.

[82] See Mark Sableman, Link Law Revisited: internet Linking Law at Five Years¸ 2001; available from: http://www.btlj.org/data/articles/vol16/sableman/sableman.pdf. See also Study on the Liability of internet Intermediaries, Markt/2006/09/E (Service Contract ETD/2006/IM/E2/69), 12 November 2007, available at http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf.

[83] Mouvement Raëlien Suisse v. Swizerland, Application no. 16354/06), 13 July 2012.

[84] Ibid.

[85] Crookes v. Newton, 2009 BCCA 392, 15 September 2009; available at http://www.courts.gov.bc.ca/jdb-txt/CA/09/03/2009BCCA0392err1.htm.

[86] The 2011 Report of the UN Special Rapporteur, op.cit. para 16.

[87] Ibid., para 18.

[88] Ibid.

[89] Ibid., para 38.

[90] Ibid., para 28.

[91] For example, the Council of Europe Convention on Cybercrime, Adopted 23.11.2001 in Budapest, does not include a definition on cybercrime, but lists offences to be criminalised by member states. See, http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG. The UN Manual on the Prevention and Control of Computer Related Crime includes fraud, forgery, and unauthorized access in its definition of computer (-related) crimes; see http://www.uncjin.org/Documents/EighthCongress.html. The NATO Parliamentary Assembly equates cyber-attacks with cybercrime, cyber terror, or cyber war, depending on the involved type of actors and motivations. See, NATO Parliamentary Assembly, 2009 Annual Session Committee Report, 173 DSCFC 09 E BIS – NATO and Cyber Defence; available at http://www.nato-pa.int/default.asp?SHORTCUT=1782.

[92] "Boot net" is term used for booting (or "jumpstart") over the network, that is a process or set of operations that loads and starts the operating system.

[93] The 2011 Report of the UN Special Rapporteur, op.cit. para 34.

[94] Resolution on the Creation of a global culture of cyber security, A/RES/57/239, Jan. 31, 2003; available at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf.

[95] Council of Europe Convention on Cybercrime, op.cit.. Preamble.

[96] Ibid. Article 27(4) (a).

[97] C.f., for example, Iran: Computer Crime Laws, 11 January 2012, available at http://www.article19.org/resources.php/resource/2922/en/iran:-computer-crimes-law; Iraq: Draft Informatics Crimes Law, 26 October 2011, available at http://www.article19.org/resources.php/resource/2792/en/iraq:-draft-informatics-crimes-law; or Brazil: Draft Computer Crime Bill, 7 September 2012; available at: http://www.article19.org/resources.php/resource/3432/en/brazil:-draft-computer-crime-bill.

[98] Recommendation CM/Rec (2011)7 on a new notion of 'media', available at https://wcd.coe.int/ViewDoc.jsp?id=1835645&Site=COE.

[99] See Press Complaint Commission website, Q&A, available at: http://www.pcc.org.uk/faqs.html#faq2_13.

[100] See Recommendation CM/Rec (2011)7, op.cit.

[101] Ibid.

[102] See, UNESCO, Communication and Information, http://portal.unesco.org/ci/en/ev.php-URL_ID=3038&URL_DO=DO_TOPIC&URL_SECTION=201.html.

[103] UN Division for Public Economics and Public Administration & the American Society for Public Administration, Benchmarking E-government: A global perspective – Assessing the progress of member states, May 2002, p. 1; available at http://unpan1.un.org/intradoc/groups/public/documents/UN/UNPAN021547.pdf. The study distinguishes between five different stages of e-government: the emerging stage where simply an official government online presence is established, the enhanced stage where information provided becomes more dynamic, the interactive stage where users can download forms, e-mail officials and interact through the web, the transactional stage that allows users to pay for services and other transactions online, and finally the seamless stage that represents a full integration of e-services across administrative borders and on all administrative levels.

[104] For example, Austria, Switzerland and some German federal states have started to open up data; see http://gov.opendata.at/site/. http://opendata.ch/, or http://opendata.service-bw.de/Seiten/default.aspx.

[105] Available at http://www.zim.mpg.de/openaccess-berlin/berlin_declaration.pdf.

[106] Ibid.

[107] Memorandum of Understanding between the U.S. Department of Commerce and internet Corporation for Assigned Names and Numbers of 25 November 1998; available at http://www.icann.org/en/about/agreements/mou-jpa/icann-mou-25nov98-en.htm.

[108] ICANN has in the meantime concluded additional memoranda of understanding with national and regional telecommunication commissions and international organisations, such as with UNESCO, the Russian Association of Networks and Services, the Inter-American Telecommunications Commission of the OAS, the African Telecommunications Union, the Commonwealth Telecommunications Organization, and the Pacific Islands Telecommunications Association. All available at http://www.icann.org/en/about/agreements/partnership-mous. In general, these memoranda are meant to foster cooperation, exchange of information and partnership building between the telecommunication unions and ICANN on issues related to internet governance. The aim is to foster the development of telecommunications and information technologies as they relate to the security and stability of the internet. With UNESCO ICANN concluded a MoU to support the introduction of top-level internationalized domain names that allow users to establish and use domains in their language-specific script.

[109] David P. Fidler, internet Governance and International Law: The Controversy Concerning Revision of the International Telecommunication Regulations, American Society of International Law – Insights, Volume 17, Issue 6, 7 February 2013.

[110] Available at http://www.itu.int/wsis/implementation/igf/index.html.

[111] Declaration of Principles, Building the Information Society: a global challenge in the new Millennium, WSIS-03/GENEVA/DOC/4-E, 12 December 2003; available at http://www.itu.int/wsis/docs/geneva/official/dop.html.

[112] Ibid.

[113] Ibid.

[114] All papers and government positions related to the WSIS in Tunis in 2005 are available at http://www.itu.int/wsis/documents/listing-all.asp?lang=en&c_event=pc2l3&c_type=all.l.

[115] See, the Proposal on internet Governance European Union (UK), WSIS-II/PC-3/DT/21, PrepCom-3, Geneva, 19-30 September 2005.

[116] Tunis Commitment, WSIS-05/TUNIS/DOC/7-E, 18 November 2005.

[117] See WSIS-05/TUNIS/DOC/6(Rev. 1)-E, 18 November 2005, para 34; available at http://www.itu.int/wsis/docs2/tunis/off/6rev1.html.

[118] Ibid, para 72.

[119] Declaration by the Committee of Ministers on internet governance principles, adopted by the Committee of Ministers on 21 September 2011 at the 1121st meeting of the Ministers' Deputies, available from: https://wcd.coe.int/ViewDoc.jsp?id=1835773.

[120] OSCE, Amsterdam Recommendations, 14 June 2003, available at http://www.osce.org/fom/41903.

[121] The 2005 Joint Declaration, op.cit.

[122] See, Tenth anniversary Joint Declaration: Ten key challenges to freedom of expression in the next decade, available at http://www.osce.org/fom/41439.

[123] The 2011 Joint Declaration, op.cit.