ARTICLE 19

Tunisia: Background paper on Internet regulation

May 2013

Legal analysis

Summary

Between February 2012 and February 2013, ARTICLE 19 analysed the state of Internet freedom in Tunisia. In particular, we examined the compatibility of the Tunisian legal framework governing the Internet against international and comparative standards for the protection of freedom of expression and the right to privacy.

Our analysis shows that the case for reform in this area is overwhelming. Indeed, the restrictions imposed on Internet usage have certainly gone backwards due to the deactivation of censoring mechanisms and the inability of the governing body exercising control over the Internet. Nevertheless, the repressive legislative and regulatory system prior to 14 January 2011, put in place by the dictatorship, is still active. It has not undergone any significant changes to guarantee freedom of speech on the Internet in an effective, sustainable and irreversible manner.

ARTICLE 19 therefore expresses its grave concerns about the persistence of certain legislative and regulatory provisions that restrict freedom of speech on the Internet. This notably affects:

The provisions of the telecommunications decree, and in particular:

- Articles 5 and 6 that entrust discretionary power to the government in matters of attributing prior authorisation for the provision of telecommunication services;
- Articles 9 and 87 relating to the conditions and procedures of usage or encryption services, and the sanction of use of these means without prior authorisation;
- Decree No 97-501 of 14 March 1997 concerning value-added telecommunications services and the Regulations of 22 March 1997 concerning the specifications for setting up and operating value-added Internet telecommunications services. This legislation is in clear breach of international law. In particular, the decree and regulations make Internet Service Providers (ISPs) liable for third-party content without any exceptions.
- Law N°2004-5 of 3 February 2004 concerning information security. This legislation was adopted, theoretically, to guarantee the security of public and private information systems and networks. In practice, however, it allows the authorities, under the guise of carrying out technical inspections, of carrying out continuous censorship of the Internet.

Furthermore, ARTICLE 19 worries about the gaps in the Tunisian legislative framework that concern the protection of the freedom of speech and the protection of one's private life on the Internet, particularly:

- The absence of a well defined legislative framework governing the listening operations (telephone tapping) and access to the content of correspondence, including electronic correspondence;
- The organic law N°2004-63 of 27 July 2004 on data protection. This law does not provide exemptions or derogations to the application of data protection provisions in the framework of the treatment of data processed for solely journalistic purposes. This gap exposes bloggers and citizen-journalists to penal sanctions in certain circumstances.
- The absence of the explicit protection in the law of principle of the Internet's neutrality.

ARTICLE 19 welcomes the absence of Internet regulations in certain areas. In particular, ARTICLE 19 believes that it is unnecessary to adopt legislation to address specific online content for the simple reason that the laws that regulate content are of general application, i.e. they apply offline and online. Similarly, there is no need to regulate bloggers and citizen-journalists other than by way of the same laws that apply to everyone else. By contrast, bloggers and citizen-journalists

should benefit from source protection, just as professional journalists do, with the objective of being able to favour the emergence of a free and responsible citizen press. At the same time, the legislation concerning data protection must unavoidably take into consideration the nature of bloggers and citizen journalists' activities.

Key Recommendations

- The provisions governing ISP liability, fixed by the Telecommunications Decree N°1997-501 and by Internet Regulations of 22 March 1997, should be removed and replaced with provisions granting immunity, and more explicitly, ISPs should not be held responsible for the publication of content produced by third parties, including their clients, where the ISPs have not intervened in this content.
- The need of stating the principle of Internet neutrality and forbidding ISPs to keep under surveillance the content circulating on their networks.
- The law should be amended to require that only the courts may grant a blocking/filtering/removal order subject to the principles of necessity and proportionality;
- Article 8 of the Internet Regulations fixed by the decree of 22 March 1997 which requires which requires ISPs to submit a list of their subscribers to the authorities on a monthly basis should be repealed;
- Article 11 of the Internet Regulations, fixed by the decree of 22 March 1997, bars the use of encryption technologies without prior approval from the authorities should be removed. The authorities should, nevertheless, be able to ask for decryption codes in the fight against criminality, to the extent that these requests fulfil the conditions of necessity and proportionality stated in Article 17 of the ICCPR.
- The need to amend the law regarding the protection of personal data in order to protect bloggers and citizen-journalists against penal sanctions planned by this law.
- Need to review Law N°2004-5 concerning information security with the view of strictly defining the term 'information security' and of limiting the powers of the National Agency of information security in matters of technical control of information systems and networks.
- Bloggers and citizen journalists should not be regulated other than by way of the same civil and criminal laws that apply to non-internet users, subject to our recommendations here-below concerning the Press Code.
- The Press Code should be amended to entitle bloggers to source protection.
- The Press Code should be amended to decriminalise defamation.
- The hate speech provisions should be more tightly drafted along the lines of ARTICLE 19's Camden Principles on Freedom of Expression and Equality, which elaborate on this issue.

About the Article 19 Law Programme

In February 2012, ARTICLE 19 analysed the state of Internet freedom in Tunisia. In particular, we examined the compatibility of the Tunisian legal framework governing the Internet against international and comparative standards for the protection of freedom of expression and the right to privacy.

The ARTICLE 19 Law Programme advocates for the development of progressive standards on freedom of expression and access to information at the international level, and their implementation in domestic legal systems. The Law Programme has produced a number of standard-setting publications which outline international and comparative law and best practice in areas such as defamation law, access to information and broadcast regulation.

On the basis of these publications and ARTICLE 19's overall legal expertise, the Law Programme publishes a number of legal analyses each year, comments on legislative proposals as well as existing laws that affect the right to freedom of expression. This analytical work, carried out since 1998 as a means of supporting positive law reform efforts worldwide, frequently leads to substantial improvements in proposed or existing domestic legislation. All of our analyses are available online at http://www.article19.org/resources.php/legal/.

If you would like to discuss this analysis further, please contact Gabrielle Guillemin, Legal Officer at gabrielle@article19.org. If you want to learn more about the work of ARTICLE 19 in Tunisia, please contact Saloua Gazhouan at saloua@article19.org.

Introduction

The Internet has radically transformed the way in which people receive and share information and ideas. It has become a basic requirement for the enjoyment of freedom of expression, which is the foundation of a democratic society. The Tunisian Revolution is a case in point.

Two and a half years after the Revolution, ARTICLE 19 believes that it is time for Tunisia to assess the state of media freedom. As the Interim Government have made the reform of the media sector a key priority, the protection of freedom of expression on the Internet cannot be ignored.

Between February 2012 and February 2013, ARTICLE 19 analysed the state of Internet freedom in Tunisia, on a legislative and practical level. In particular, we examined the compatibility of the Tunisian legal framework governing the Internet against international and comparative standards for the protection of freedom of expression, and the right to privacy.

This document is a critical analysis of the state of Internet freedom in Tunisia. It proceeds from a comprehensive approach that consists in verifying the compatibility of Tunisian legislation in this domain. On this point, ARTICLE 19 bases itself on its extensive expertise in the defence of freedom of speech throughout the world in general and more specifically, in Tunisia. In fact, ARTICLE 19 had published critical analyses of several draft decrees adopted in Tunisia, including:

- The Draft Decree relating to Freedom of the Press, of printing and editing
- Decree on the Freedom of Audiovisual Communication and the Creation of an Independent Higher Authority for Audiovisual Communication of Tunisia
- The Draft Decree on Access to Administrative Documents
- The Draft Election law

Our analysis shows that the case for reform in this area is overwhelming. While the Internet may be partly free in practice since the ousting of President Ben Ali, the repressive laws that formed part of the censorship apparatus of his government remain. There is therefore a real danger that free speech on the Internet may be stifled again as long as they are still on the statute book.

In light of our concerns outlines above, this paper seeks to assist Tunisian legislators, the Interim Government, human rights campaigners and other Internet stakeholders, in examining how best to ensure the protection of Internet freedom in Tunisia. In particular, it sets out specific recommendations on how this could be achieved.

The paper is divided into three sections.

Section I briefly sets out the state of Internet freedom in Tunisia.

Section II lays down applicable international standards on the protection of freedom of expression online.

Section III examines the Tunisian legal framework governing free of expression on the Internet against those standards and makes a number of recommendations for reform in this area.

Internet freedom in Tunisia

The study on the state of Internet freedom in Tunisia requires a comparison between the situation under the Ben Ali regime and the post-revolutionary situation.

I. Gagging Internet Freedom under President Ben Ali

On 17 December 2010, Mohamed Bouazizi, a young fruit seller, set himself on fire in the town of Sidi Bouzid in protest against the confiscation of his wares by police and subsequent humiliation inflicted on him by municipal officials. This event sparked an unprecedented wave of protests throughout the country eventually leading to the ousting of its long-term President Ben Ali.

Under the Ben Ali regime, media censorship was widespread. The Internet was therefore a comparatively more open forum for the exchange of information and opinions about social and political issues. It is widely believed that Bouazizi's death and popular uprising that ensued would not have attracted the world's attention without social media sites such as Facebook, Twitter and YouTube, showing images of the demonstrations and the use of force by police against peaceful protesters.

The Internet was not free under President Ben Ali, however. His government had put in place a sophisticated, multilayered, Internet filtering system which was regarded as one of the most repressive in the world. According to Freedom House, the government used three techniques as part of its Internet censorship strategy: technical filtering, post-publication deletion and takedown, and proactive manipulation of public opinion online.

In particular, the Tunisian Internet Authority (also known under its French acronym 'ATI') – which controls the Internet backbone in Tunisia - was tasked with implementing the country's Internet filtering system at network level. Moreover, as the authority in charge of domain name registration, the ATI was able to remove entire domains at will. A number of other technical tools were used to block access to websites deemed undesirable by the authorities.

The government further issued instructions to ISPs on what types of content should be blocked or otherwise removed: pornography, anti-government speech, discussions of human rights in Tunisia, and Internet censorship circumvention tools or technology. In 2010, an upsurge in the number of arbitrary blocking was reported. For example, applications such as the file-sharing site Flickr and YouTube were temporarily blocked in 2010.

Furthermore, online journalists and bloggers were routinely arrested on trumped up charges such as harassment or assault, whilst some internet users were arbitrarily detained and questioned.

Notably, this was the case of cyber dissident, Zouheir Yahyaoui, administrator of the site « Tunezine » (www.tunezine.com) and the first Arab and African blogger to be imprisoned for what he wrote on the Internet.

In its policies targeted at controlling the freedom of Internet expression, the Tunisian state relied on large amount of legal documents that ARTICLE 19 consider as repressive and restrictive. This legislation and regulations are:

- The provisions of the telecommunications decree and, in particular:

• Articles 5 and 6 that entrust discretionary power to the government in terms of the attribution of prior authorisation for the provision of telecommunication services. The fact of entrusting these discretionary powers to the public authorities allows them, even in a direct manner, of controlling the freedom of individuals to access the Internet network;

• Articles 9 and 87 concerning the procedures of use of the encryption means or services and the sanction of the usage of these means with prior authorisation;

- Law N°2004-5 of 3 February concerning computer security. This legislation was adopted, theoretically, to guarantee the security of private and public information networks. However, in practice, it allowed the authorities, under the premise of technical control, to carry out continuous censorship of the Internet under the Ben Ali regime. Article 3 of this law entrusts the National Agency for Computer Security (known in French as ANSI) general control over public and private computer systems and networks, and the supervision of the implementation of national strategies in this domain. In the absence of a precise definition of the notion of computer security, the legislators gave the government the power to entrust ANSI of carrying out all activities relating to the domain of intervention. The general nature of this law and the wide powers attributed to ANSI threaten freedom of expression, and more notably what relates to opportunities for content filtering.

- Decree no.97-501 of 14 March 1997 concerning valued added telecommunication services and the decree of 22 March 1997 regarding the implementation and exploitation of valued added telecommunication Internet services. This legislation is incompatible with international standards as it renders ISPs entirely responsible for the circulation of content produced by third parties. They impose on them the obligation of controlling and removing all content contrary to public order and 'good morals', and oblige them to submit to the public operator, that is to say the Tunisian Internet Authority, a list of all their subscribers at the beginning of each month.

- The organic law N°2004-63 of 27 July 2004 on the protection of personal data. Initially this law was announced to restore the image of the Ben Ali regime which was getting ready to host the second phase of the World Summit on the Information Society (WSIS) and to undermine the criticism of the international community against its repressive practices. However, the law does not provide exemptions or derogations to the application of provisions of protection of data in the framework of the treatment of data processed for journalistic, artistic, literary or cultural purposes. This gap exposes bloggers and citizen-journalists to criminal sanctions in certain circumstances. Furthermore, guaranteeing the protection of personal data, with the consent of the person concerned, is not applied to personal data processed by the public authorities – this can lead to bloggers and citizen-journalists to censor themselves, for fear of being prosecuted by the authorities.

Finally, it must be noted that a well-defined legal framework governing listening operations and access to the content of correspondence, including electronic correspondence, to fight against criminality and protect national security, has long allowed the Ben Ali regime to exercise continuous surveillance in Tunisia.

II. Internet Freedom after the Revolution

A few hours before the fall of his regime, President Ben Ali delivered a final speech to public opinion in which he notably announced the easing of censorship of the Internet network. All websites suddenly became accessible. The transitional government, which took power after 14 January 2011, approved this choice and put an end to the government's censorship.

However, ARTICLE 19 is concerned about the future of freedom of speech on the Internet in Tunisia with regards to certain indications that show that censorship of the Internet has not totally disappeared. Among these indications, Article 19 particularly recalls:

- a decision of the Court of Appeal of 15 August 2011 to prohibit access to pornographic content. The court ordered ATI to implement a filtering system to prevent access to such content. Nawaat, a Tunisian blogging group, thus recently questioned whether one year after the Revolution, '#Ammar404' (codename for ATI) may be coming back. Similarly, Reporters without Borders reported on the return of Internet filtering practices.

The Court of Cassation subsequently overturned the Court of Appeal's judgment on appeal from ATI. However, this has failed to assuage the fears of many Tunisians that censorship may be coming back for the three following reasons:

1- the Court of Appeal's decision was quashed merely on technical grounds: the decision of the Court of Cassation was based on the principle of incompetence of judiciary justice to deal with these types of disputes that fall rather under administrative justice.

2- in its statements of reasons, the Court of Cassation based itself on the ministerial communications decree of 22 March 1997 concerning the specifications and conditions of use for operating value-added Internet telecommunications services. The Court concluded that the ATI has the right to exercise administrative control on the Internet, to ban the dissemination by suppliers or users of content offensive to public order or good morals. According to the Court of Cassation, the ATI would therefore have the right to take measures to protect public order and to restrict individuals' freedom of accessing the Internet. The Court of Cassation implicitly considers that that the ATI has the power to filter or block certain websites, if the Administrative Tribunal deems so. Ultimately, as long as the question of legal jurisdiction is reviewed for one reason or another, the ATI will have, under the guise of protecting public order, the obligation of filtering or blocking certain electronic sites. Yet the concept of "public order" is a very vague, very large and progressive notion in accordance with traditions, social practices and religious beliefs. Consequently, requiring the filtering of pornographic websites and entrusting this mission to the ATI risks leading to the filtering of all sites that do not suit the public authorities, certain social groups or even certain individuals.

An obvious concern is that Internet filtering may be expanded to other types of content and this is especially so as the protection of freedom of expression in Tunisia remains fragile in the face of the country's religious and moral values. The prosecution of TV executive Nabil Karoui for blasphemy following the broadcast of Persepolis, the award-winning animated film about the 1979 Iranian revolution is a paradigmatic example. The film was criticised for showing a representation of God, which is not allowed by Islam.

3- The legal framework which allows the control and censorship of the Internet is active after the fall of President Ben Ali's regime, notably on the basis of its active legislation by a military examining judge who ordered that the ATI filter Facebook pages judged as hostile by the institution of the army. Faced with ATI's technical inability of proceeding with such an operation that risked having a negative effect on the quality of services provided by other ISPs, and following discussions between the ATI and military justice, the inefficiency and the impossibility of

maintaining the blockage quickly became evident. From this point forward, these pages are accessible.

Many other requests for filtering or blocking sites or removal of Facebook pages were addressed to ATI by persons or institutions. This was notably so with case N°289 of 4 July 2011 between the ATI and the gene bank. In this matter, the national gene bank asked ATI to close a Facebook page administered by an individual and containing criticism against the institution. The court of the first body refused to agree to this request, considering that the criticism made on this Facebook page fell under freedom of expression. This decision was confirmed by the Court of Appeal (Case N°26217 of 24 November 2011) that specified, nevertheless, that the author of this page could be prosecuted for the dissemination of spreading false news and defamation.

In two preceding cases show that the courts, in theory, do not refuse to judge the requests for filtering and blockage of internet sites, that freedom to surf the net and freedom of internet expression is guaranteed and that accepting requests for blocking or filtering websites is conditioned by the respect for the right of freedom of expression, a fundamental right.

Jurisprudence in Tunisia heads towards the appropriation of international standards that have, nonetheless, a certain extrapolation in the definition of conditions of filtering and blockage, in relation to concepts of public order and good morals. In the case of filtering pornographic sites, the Court of Appeal indicated that in its decision "the absolute freedom of navigating the internet and accessing all sites, including pornographic sites, as a direct consequence causes the loss of certain necessary moral values for the education of young generations, and to building a healthy and balanced society, especially that filtering pornographic sites does not necessarily lead to the filtering of scientific or other sites".

This jurisprudence is based on a legal and judicial system inherited from the ancient former regime that still remains active despite the suspension of the 1959 constitution.

Despite the consensus that came about, at least on the level of speech, around the necessity of reforming the information system, the question of the protection of freedom of expression on the Internet did not receive all the necessary attention.

Acts of violence recorded in the last two and a half years, reached their height with the murder of a militant and political opponent on 6 February 2013. They have restored to the agenda the matter of Internet freedom of expression due to the increase in hate speech and violence on the social networks. These voices were, in fact, raised to control the freedom of expression on the Internet.

All requests for filtering or blocking have been addressed, until now, to ATI, in its role of as national operator and no requests have been addressed to the ISPs who are, however, also able to do this. Nevertheless, the minister of communications concluded at the start of 2013, an agreement with the ISPs, in virtue of which the latter are henceforth conferred to pass via the ATI for everything that concerns connection to and surfing of the net. For various reasons, such an agreement risks instituting multiple supervision carried out by the different ISPs. These ISPs can also succumb to diktats of politic power that hold many means of pressuring the ISPs, whilst the ATI is a public institution, governed by active legislation that, theoretically, is sheltered from political pressures.

The difficulty of making decisions to censor the Internet must also be noted. The ATI repeatedly confirms that it finds itself technically incapable of making these decisions. Additionally, censorship can cause disruption to the normal access of sites and non-censored pages.

Finally, it must be noted that the recent use of the organic law N°2004-63 concerning the protection of personal data as a remedy against certain embarrassing remarks by bloggers. More particularly, it regards the complaint made by the Tunisian minister of Foreign Affairs against the blogger Olfa Riahi, in January 2013. The complaint was lodged based on numerous texts such as articles 89 and 90 of the organic law N°2004-63 concerning the protection of personal data. The blogger in question had raised suspicions about a relationship between the minister and one of his relatives by mentioning that the latter had spent a night in the same hotel as the minister.

International standards on Internet Freedom

In February 2012, ARTICLE 19 analysed the state of Internet freedom in Tunisia. In particular, we examined the compatibility of the Tunisian legal framework governing the Internet against international and comparative standards for the protection of freedom of expression and the right to privacy.

The rights to freedom of expression and information are fundamental and necessary conditions for the realisation of the principles of transparency and accountability that are, in turn, essential for the promotion and protection of all human rights in a democratic society. This section identifies international and regional standards for the protection of these rights, in particular in relation to the regulation of online content, the rights of bloggers and citizen journalists, the liability of Internet Service Providers (ISPs), surveillance, cyber security and access to the Internet. These standards form the basis of our recommendations on how best to protect freedom of expression on the Internet in Tunisia, which are set out in Section III below :

I. The founding principles of freedom of expression

A - Universal Declaration of Human Rights

Article 19 of the Universal Declaration of Human Rights (UDHR)[1] 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 its adoption in 1948.[2]

B - International Covenant on Civil and Political Rights

The International Covenant on Civil and Political Rights (ICCPR) elaborates upon and gives legal force to many of the rights articulated in the UDHR. The ICCPR binds its 167 states party to respect its provisions and implement its framework at the national level.[3] Tunisia ratified the ICCPR on 18 March 1969 and is therefore legally bound to respect and to ensure the right to freedom of expression as contained in Article 19 of the ICCPR:

> 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

[1] UN General Assembly Resolution 217A(III), adopted 10 December 1948.

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

[3] Article 2 of the ICCPR, GA res. 2200A (XXI), 21 UN GAOR Supp. (No. 16) at 52, UN Doc. A/6316 (1966); 999 UNTS 171; 6 ILM 368 (1967).

> 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 ('HRC'), as treaty monitoring body for the ICCPR, issued General Comment No 34 in relation to Article 19.[4] General Comment No.34 constitutes an authoritative interpretation of the minimum standards guaranteed by Article 19 ICCPR. ARTICLE 19 considers General Comment No 34 to be a progressive clarification of international law related to freedom of expression and access to information.[5] It is particularly instructive on a number of issues relative to freedom of expression on the Internet.

Importantly, General Comment No 34 states that Article 19 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, the legal framework regulating the mass media should take into account the differences between the print and broadcast media and the Internet, while also noting the ways in which media converge.[8]

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 that regulatory approaches in the telecommunications and broadcasting sectors cannot simply be transferred to the Internet.[9] In particular, they recommend the development of tailored approaches for responding to illegal content online, while pointing out that specific restrictions for material disseminated over the Internet are unnecessary.[10] They also promote the use of self-regulation as an effective tool in redressing harmful speech.[11]

As a state party to the ICCPR, Tunisia must ensure that any of its laws attempting to regulate electronic and Internet-based modes of expression comply with Article 19 ICCPR as interpreted by the UN Human Rights Committee and that they are in line with the special mandates' recommendations.

II. 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.

---

[4] See, CCPR/C/GC/3 available from: http://www2.ohchr.org/english/bodies/hrc/comments.htm

[5] ARTICLE 19 statement on UN Human Rights Committee Comment No.34

http://www.article19.org/resources.php/resource/2631/en/un:-article-19-welcomes-general-comment-on-freedom-ofexpression

[6] UN Human Rights Committee General Comment No.34, para. 12.

[7] Ibid., para. 17.

[8] Ibid., para. 39.

[9] See Joint Declaration on Freedom of Expression and the Internet, June 2011, available at:

http://www.article19.org/data/files/pdfs/press/international-mechanisms-for-promoting-freedom-of-expression.pdf

[10] Ibid.

[11] Ibid.

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. It is required that restrictions are: (i) provided by law; (ii) pursue a legitimate aim; and (iii) that they conform to the strict tests of necessity and proportionality.[12]

i) "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.[13] Ambiguous or overly broad restrictions on freedom of expression are therefore impermissible under Article 19(3).

ii) "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.[14] 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.

iii) "Necessity"

States party to the ICCPR are obliged to ensure that legitimate restrictions on the right to freedom of expression are necessary and proportionate. Necessity requires 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 if a less intrusive measure is capable of achieving the same purpose as a more restrictive one, the least restrictive measure must be applied.

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

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

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

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

> 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.[15]

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 a recent report dated 10 August 2011.[16] In that report, the Special Rapporteur also clarified the scope of legitimate restrictions on different types of expression online. This is examined in more detail further below.[17]

III. 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 its cultural, moral or religious traditions, online content regulation has become an important focus of 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.[18] In his report of 10 August 2011, the UN Special Rapporteur identified three different types of expression for the purposes of online regulation: (i) expression that constitutes an offence under international law and can be prosecuted criminally; (ii) expression that is not criminally punishable but may justify a restriction and a civil suit; and (iii) expression that does not give rise to criminal or civil sanctions, but still raises concerns in terms of tolerance, civility and respect for others.[19]

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 further made clear that even legislation criminalising these types of expression must be sufficiently precise, and there must be adequate and effective safeguards against abuse or misuse, including oversight and review by an independent and impartial tribunal or regulatory body.[20] In other words,

---

[15] Concluding observations on the Syrian Arab Republic (CCPR/CO/84/SYR).

[16] See UN Special Rapporteur on Freedom of Expression, A/66/290, 10 August 2011, para. 16:

http://www.ohchr.org/Documents/Issues/Opinion/A.66.290.pdf

[17] Ibid., para. 18.

[18] See note 35, ibid.

[19] Ibid.

[20] Ibid, para. 22

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 expression online must be unambiguous, pursue a legitimate purpose and 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 regarding the necessity and justification for blocking a particular website, stressing that "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".[21]

Finally, the Special Rapporteur has highlighted that all other types of expression, such as defamatory comments, should not be criminalised. Rather, States should promote the use of more 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 online derogatory comments almost immediately 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.[22]

IV. The rights of citizen-journalists and bloggers

The advent of the Internet means that any individual can now self-publish his opinions and ideas on a blog or social media network. This raises the question of how journalism should be defined and what is 'media' in the digital age. Equally, the question arises 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 on the international level. Nonetheless, the UN Human Rights Committee and the Council of Europe have provided tentative responses, which we set out further below. As far as the question of regulation is concerned, it is clear that bloggers and citizen journalists should not be required to register, let alone register under their real name under international law (see section on Surveillance below). 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 avail themselves of the protection of sources.

A - Definition of journalism and new media

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

[21] Ibid. Para. 38

[22] See UN Special Rapporteur on Freedom of Expression, A/HRC/17/27, 16 May 2011, para. 28

> 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 thus taken a functional approach to the definition of journalism. In other words, journalism is an activity, which consists in the collection and dissemination of information to the public via any means of mass communication.

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:[23]

- **adopt 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 that should be taken into account when trying to determine whether a particular activity or actors 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; (iv) outreach and dissemination; and (v) public expectation.

In addition, the Committee provided a set of indicators in 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 it 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 criterion should be applied flexibly.

Interestingly, the Committee said that bloggers should only be considered media if they meet certain professional standards criteria to a sufficient degree. It is instructive 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.[24] The Press and

[23] The Recommendation is available here: https://wcd.coe.int/ViewDoc.jsp?id=1835645&Site=COE

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

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 nonjournalists". 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.

B/ 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 made subject to registration or licensing requirements. Similarly, they should be accredited only where 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*".[25] 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 such laws, e.g. defamation law. Nonetheless, the question arises whether bloggers and citizens should benefit from the same legal protections as journalists where they undertake the activity of journalism.

Legal protection

There are no set international legal standards concerning the legal protection to 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 equally afford themselves of the defences available in the law. The question 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).

[25] See Recommendation CM/Rec (2011)7 on a new notion of 'media' cited above.

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 further recommended that some form of support and protection should be provided to media actors who do not fully qualify as media under a number of criteria set forth by the Committee, such as bloggers, but who at the same time 'participate in the media ecosystem'.[26]

V. Role of Internet intermediaries and intermediary liability

Intermediaries, such as Internet Service Providers (ISPs), search engines, social media platforms and web hosts, play a crucial role in relation to access to the Internet and transmission of third party content. They have come to be seen as the gatekeepers of the Internet. For Internet activists, they are key enablers of the meaningful exercise of the right to freedom of expression, facilitating the free flow of information and ideas worldwide, while law enforcement agencies view them as central to any strategy to combat online criminal activity.

Given the huge amount of information that is available on the Internet, and that could potentially be unlawful, e.g. copyright law, defamation laws, hate speech laws, criminal laws for the protection of children against child pornography, Internet intermediaries have had a strong interest in seeking immunity from liability on the Internet.

In many western countries, Internet intermediaries have been granted immunity for third - party content, whether as hosts, mere conduits, or for caching information. 46 They have also been exempted from monitoring content.[27] However, when acting as hosts, they have been made subject to **'notice and take - down' procedures**, which require them to remove content once they are put on notice by private parties or law enforcement agencies that a particular content is unlawful. This system can be found for example in the E - commerce directive in the EU and the Digital Copyright Millennium Act 1998 (the so - called 'safe harbours') in the US.

A number of problems have been identified in relation to such 'notice and take-down' procedures. First, they often lack a clear legal basis. For example, a recent OSCE report on Freedom of Expression on the Internet highlights that:[28]

> Liability provisions for service providers are not always clear and complex notice and takedown provisions exist for content removal from the Internet within a number of participating States. Approximately 30 participating States have laws based on the EU E-Commerce Directive. However, the EU Directive provisions rather than aligning state level policies, created differences in interpretation during the national implementation process. These differences emerged once the provisions were applied by the national courts. Aware of such issues, the European Commission launched a consultation during 2010 on the interpretation of the intermediary liability provisions. A review report is expected during 2011.

---

[26] See n 44 above.

[27] See Article 15 of the E-commerce directive. In the recent case of *SABAM* v. *Scarlet Extended SA*, the Court of Justice of the European Union (CJEU) considered that an injunction requiring an ISP to install a filtering system to make it absolutely impossible for its customers to send or receive files containing musical works using peer-to-peer software without the permission of the rights holders would oblige it to actively monitor all the data relating to each of its customers, which would be in breach of the right to privacy and the right to freedom to receive or impart information. The court noted that such an injunction could potentially undermine freedom of information since the suggested filtering system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications.

[28] OSCE report, Freedom of Expression and the Internet, July 2011, p 30.

Moreover, **these procedures lack procedural fairness**: rather than obtain a court order requiring the ISP to remove unlawful material (which, in principle at least, would involve an independent judicial determination that the material is indeed unlawful), ISPs are required to act merely on the say-so of a private party or public body. This is problematic because intermediaries tend to err on the side of caution and take-down material which may be perfectly legitimate and lawful. As the UN Special Rapporteur on freedom of expression recently noted:[29]

> 42. [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 overcensoring potentially illegal content. Lack of transparency in the intermediaries' decision-making process also often obscures discriminatory practices or political pressure affecting the companies' decisions. 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.

Accordingly, the four special rapporteurs on freedom of expression recommended in their 2011 Joint Declaration on Freedom of Expression and the Internet that:

> (i) No one should be liable for content produced by others when providing technical services, such as providing access, searching for, or transmission or caching of (i) information;[30]
>
> (ii) Liability should only be incurred if the intermediary has specifically intervened in the content, which is published online;[31]
>
> (iii) ISPs and other intermediaries should only be required to take down content following a court order, contrary to the practice of notice and takedown.[32]

Similarly, the UN Special Rapporteur on freedom of expression has stated that "*censorship measures should never be delegated to a private entity, and that no one should be held liable for content on the Internet of which they are not the author. Indeed, no State should use or force intermediaries to undertake censorship on its behalf*".[33] He has further recommended that in order to avoid infringing the right to freedom of expression and the right to privacy, intermediaries should:[34] [O]nly implement restrictions to these rights after judicial intervention; be transparent to

[29] See UN Special Rapporteur on Freedom of Expression report, cited above at n 41, para. 42.

[30] See n 28 above.

[31] See n 28 above, ibid.

[32] Ibid.

[33] See UN Special Rapporteur on FOE report, cited above at n 41, para. 43.

[34] Ibid. para 47.

the user involved about measures taken, and where applicable to the wider public; provide, if possible, forewarning to users before the implementation of restrictive measures; and minimize the impact of restrictions strictly to the content involved.

Finally, the Special Rapporteur has emphasised the need for effective remedies for affected users, including the possibility of appeal through the procedures provided by the intermediary and by a competent judicial authority.[35]

VI. Surveillance of communications

Guaranteeing the right to privacy in online communications is essential for ensuring that individuals have the confidence to freely exercise their right to freedom of expression. The mass-surveillance of online communications therefore poses significant concerns for both the right to privacy and the right to freedom of expression.

The right of private communications is strongly protected in international law, through Article 17 of the ICCPR, which states that:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

In General Comment no. 16 on the right to privacy, the UN Human Rights Committee clarified that:

> 3. The term "unlawful" means that no interference can take place except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant.

The Committee went on to explain that:

> 4. The expression "arbitrary interference" is also relevant to the protection of the right provided for in article 17. In the Committee's view the expression "arbitrary interference" can also extend to interference provided for under the law. The introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances.

The Committee further stated that:

> 8. Even with regard to interferences that conform to the Covenant, relevant legislation must specify in detail the precise circumstances in which such interferences may be permit ted. A decision to make use of such authorized interference must be made only by the authority designated under the law, and on a case-by-case basis.

The UN Special Rapporteur on promotion and protection of human rights and fundamental freedoms while countering terrorism has argued that like restrictions on the right to freedom of

[35] Ibid

expression under Article 19, restrictions of the right to privacy under Article 17 of the ICCPR should be interpreted as subject to the three-part test:[36]

> [A]rticle 17 of the Covenant should also be interpreted as containing the said elements of a permissible limitations test. Restrictions that are not prescribed by law are "unlawful" in the meaning of article 17, and restrictions that fall short of being necessary or do not serve a legitimate aim constitute "arbitrary" interference with the rights provided under article 17.

The Special Rapporteur further defined the scope of legitimate restrictions on the right to privacy as follows:[37]

> States may make use of targeted surveillance measures, provided that it is case - specific interference, on the basis of a warrant issued by a judge on showing of probable cause or reasonable grounds. There must be some factual basis, related to the behaviour of an individual, which justifies the suspicion that he or she may be engaged in preparing there must be " on the basis of a warrant issued by a judge on showing of probable cause or reasonable grounds. There must be some factual basis, related to the behaviour of an individual, which justifies the suspicion that he or she may be engaged in preparing a terrorist attack."

The lack of ability of individuals to communicate privately substantially affects their freedom of expression rights. In his report of 16 May 2011, the UN Special Rapporteur on Freedom of Opinion and Expression expressed his concerns that:

53. [T]he Internet also presents new tools and mechanisms through which both State and private actors can monitor and collect information about individuals' communications and activities on the Internet. Such practices can constitute a violation of the Internet users' right to privacy, and, by undermining people's confidence and security on the Internet, impede the free flow of information and ideas online.

The UN Special Rapporteur on Freedom of Expression further noted that:

> 59. [T]he right to privacy can be subject to restrictions or limitations under certain exceptional circumstances. This may include State surveillance measures for the purposes of administration of criminal justice, prevention of crime or combating terrorism. However, such interference is permissible only if the criteria for permissible limitations under international human rights law are met. Hence, there must be a law that clearly outlines the conditions whereby individuals' right to privacy can be restricted under exceptional circumstances, and measures encroaching upon this right must be taken on the basis of a specific decision by a State authority expressly empowered by law to do so, usually the judiciary, for the purpose of protecting the rights of others, for example to secure evidence to prevent the commission of a crime, and must respect the principle of proportionality.

[36] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, A/HRC/13/37, 28 December 2009.

[37] Ibid., para. 21

In particular, the Special Rapporteur recommended that States should ensure that individuals can express themselves anonymously online and to refrain from adopting real-name registration systems.[38]

5 VII. Cybersecurity and Respect for Human Rights

International instruments and resolutions on cybersecurity recognise the importance of balancing security imperatives with fundamental human rights, in particular the right to freedom of expression.

The main international instrument dealing with Cybercrime is the Council of Europe Convention on Cybercrime ETS No. 185. The Convention was adopted in Budapest on 23 November 2001. With 32 states party, the convention has the largest membership of any international legal instrument on this topic. Membership is also open to non - Council of Europe member states. For example, the US ratified the convention in 2006.

The Cybercrime Convention is noteworthy in that it only provides for limited content - related offences, namely offences related to child pornography (Article 9) and offences related to copyright infringement (Article 10). Moreover, while law enforcement agencies are given broad investigative powers in relation to those crimes and other offences committed by means of a computer system, any such power and related procedures must conform to the requirements of the European Convention on Human Rights as interpreted by t he European Court of Human Rights. Article 15 thus provides:

> **Article 15 – Conditions and safeguards**
>
> 1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.
>
> 2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia*, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.
>
> 3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

In addition, the UN General Assembly Resolution on the "Creation of a global culture of cyber security"[39] states that "security should be implemented in a manner consistent with the values

[38] See n 41, ibid, para 84.

[39] See A/RES/57/239, Jan. 31, 2003; available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf

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."

VIII. Access to the Internet and network neutrality

A - Access to the Internet

The Internet has become a basic requirement for the exercise of freedom of expression. It is also necessary for the meaningful exercise of other rights and freedoms, such as freedom of assembly. States are therefore under a positive obligation to promote and facilitate access to the Internet. The UN Special Rapporteur on Freedom of Expression, Frank La Rue, thus recently stated: [40]

> Given that the Internet has become an indispensable tool for realizing a range of human rights, combating inequality, and accelerating development and human progress, ensuring universal access to the Internet should be a priority for all States.

The Special Rapporteur recommended that States should draw up concrete policies involving all stakeholders with a view to ensuring universal access, i.e. make the Internet widely available, accessible and affordable to all segments of the population. In particular, he suggested that States should work in partnership with the private sector to ensure Internet connectivity in all inhabited localities, including in remote rural areas. He further noted that States could subsidise Internet services and low.

Similarly, the four special mandates on freedom of expression have articulated a number of principles in relation to access to the Internet in their 2011 Joint Declaration on Freedom of Expression and the Internet, which reads as follows:

> 6. Access to the Internet
>
> a. Giving effect to the right to freedom of expression imposes an obligation on States to promote universal access to the Internet. Access to the Internet is also necessary to promote respect for other rights, such as the rights to education, health care and work, the right to assembly and association, and the right to free elections.
>
> b. Cutting off access to the Internet, or parts of the Internet, for whole populations or segments of the public (shutting down the Internet) can never be justified, including on public order or national security grounds. The same applies to slow-downs imposed on the Internet or parts of the Internet.
>
> c. 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.
>
> d. Other measures which limit access to the Internet, such as imposing registration or other requirements on service providers, are not legitimate unless they conform to the test for

[40] See UN Special Rapporteur on Freedom of Expression report of 10 August 2011, cited above at n 35.

restrictions on freedom of expression under international law.

e. States are under a positive obligation to facilitate universal access to the Internet. At a minimum, States should:

- Put in place regulatory mechanisms – which could include pricing regimes, universal service requirements and licensing agreements – that foster greater access to the Internet, including for the poor and in 'last mile' rural areas.
- Provide direct support to facilitate access, including by establishing community-based ICT centres and other public access points.
- Promote adequate awareness about both how to use the Internet and the benefits it can bring, especially among the poor, children and the elderly, and isolated rural populations.
- Put in place special measures to ensure equitable access to the Internet for the disabled and for disadvantaged persons.

f. To implement the above, States should adopt detailed multi-year action plans for increasing access to the Internet which include clear and specific targets, as well as standards of transparency, public reporting and monitoring systems.

From a comparative perspective, it should also be noted that some western countries have expressly recognised a right of access to the Internet in their national legislation or otherwise. For example, the French Conseil constitutional declared that Internet access was a fundamental right in 2009. In Finland, a decree was passed in 2009 which provides that every Internet connection needs to have a speed of at least one Megabit per second. Access to the Internet is also recognised as a basic human right in Estonia since 2000.

B - Network neutrality

An important component of the right of access to the Internet is the principle of 'network neutrality' or 'net neutrality'. It protects the right of consumers to access the content, applications, services and hardware of their choice without restrictions by Internet Service Providers (ISPs) or governments.

The principle of net neutrality requires that all Internet traffic should be treated equally, i.e. without discrimination based on content, device, author, origin or destination of the content, service or application. This means that Internet Service Providers (ISPs) or governments should not be allowed to use their control over the infrastructure of the Internet or their market power to block content, or prioritise, or slow down access to certain applications or services, such as peer-to-peer transmission.

In other words, net neutrality is essential to preserve the infrastructure and the openness of the Internet. It is also essential for the sharing of information and ideas on the Internet as protected under international human rights law. For this reason, the four special rapporteurs on freedom of expression adopted a set of principles in relation to network neutrality in their 2011 Joint

Declaration on Freedom of Expression and the Internet. In particular, they declared the following:[41]

Network Neutrality

a. 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.

b. 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.

The adoption of any net neutrality rules at domestic level should reflect these standards. In this regard, the recent Chilean law on network neutrality offers a positive example in that it provides fairly comprehensive safeguards against discriminatory practices by ISPs.[42]

In particular, it is important to ensure that there are sufficient safeguards against discrimination between different types of Internet services, such as fixed and mobile broadband. For example, ARTICLE 19 criticised the rules adopted by the US Federal Communications Commission in December 2010, as they failed to provide sufficient safeguards in that respect.[43] The European Union is currently considering the adoption of net neutrality rules.

[41] See 2011 Joint Declaration cited above at n 28.

[42] See http://www.subtel.gob.cl/prontus_subtel/site/artic/20100826/pags/20100826145847.html

[43] To read more about ARTICLE 19's concerns with the FCC rules, please go to: http://www.article19.org/resources.php/resource/2824/en/net-neutrality:-stronger-rules-needed-in-us-and-eu

Protecting Internet freedom in Tunisia

– the way forward

This part examines six major areas related to Internet freedom which should be reformed by the Interim Government in order to comply with Tunisia's obligations under the ICCPR. These include:

- the scope of the protection of Internet freedom in the Constitution,
- the regulation of online content,
- the regulation of bloggers and citizen journalists,
- liability of Internet service providers,
- surveillance
- access to the Internet and network neutrality.

I. The Constitution and freedom of expression on the Internet

The right to freedom of expression was previously protected under Article 8 of the Tunisian Constitution of 1959. Understandably, this article did not make any reference to the Internet or any other information and communication technology. The Constitution was suspended in March 2011 by Tunisia's Interim Government and a Constituent Assembly was elected and tasked with the drafting a new Constitution as part of the democratic transition of the country. This is therefore a perfect opportunity for the drafters of the new Constitution to adopt modern provisions for the protection of freedom of expression that take into account new information and communication technologies, especially the Internet.

ARTICLE 19 has already made a number of recommendations as to the types of provisions that the new Constitution should include so as to offer the strongest protection possible to the right to freedom of expression and freedom of information.[44]

In particular, we recommended that the Constitution should recognise the right of access to the Internet following the lead of a growing number of countries that have formally recognised access to the Internet as a basic human right. This paper can only reiterate the recommendation that has already been made and refer to the applicable international standards on access to the Internet mentioned above. In addition, we recommend that the Constitution should protect freedom of expression in a technology-neutral way.

Recommendations:

- Recognise the right of access to the Internet in the Constitution.
- Make the protection of freedom of expression technology-neutral in the Constitution.
- Extend the provisions of the proposed draft of the constitution to the freedom of opinion, and express and state the principle that the content of the restrictions must comply with international standards and respond to, in any case, the principles of necessities and proportionalities.

[44] See ARTICLE 19, Tunisia: Protecting Freed on of Expression and Freedom of Information in the New Constitution, March 2012 (unpublished).

II. **Regulation of online content**

To ARTICLE 19's knowledge, Tunisia has not adopted a law that specifically regulates online content. This is in line with the legislation of most democracies, which only tend to have separate laws to deal with defamation, hate speech, incitement to terrorism and so forth. These laws apply to all forms of expression regardless of the media.

Similarly, international standards for the protection of freedom of expression apply to content, whether in print, broadcast or online. In this regard, we refer to the International Standards section above on online content regulation. In particular, we draw attention to the following recommendations of the UN Special Rapporteur on Freedom of Expression:

- 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;
d) incitement to terrorism;

- Legislation criminalising these types of expression must be sufficiently precise, and there must be adequate and effective safeguards against abuse or misuse, including oversight and review by an independent and impartial tribunal or regulatory body;

- Hate speech laws targeting expression online must be unambiguous, pursue a legitimate purpose and respect the principles of necessity and proportionality;

- Defamation should be decriminalised;

- Other speech offences, such as the dissemination of false news or information, should be decriminalised.

In relation to online child pornography, ARTICLE 19 notes that the COE Convention on Cybercrime provides useful guidance as to the way in which this offence may be formulated. In particular, Article 9 provides:

> **Article 9 – Offences related to child pornography**
>
> 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:
>
> a. producing child pornography for the purpose of its distribution through a computer system;
>
> b. offering or making available child pornography through a computer system;
>
> c. distributing or transmitting child pornography through a computer system;
>
> d. procuring child pornography through a computer system for oneself or for another person;
>
> e. possessing child pornography in a computer system or on a computer-data storage medium.
>
> 2. For the purpose of paragraph 1 above, the term "child pornography" shall include

pornographic material that visually depicts:

a. a minor engaged in sexually explicit conduct;

b. a person appearing to be a minor engaged in sexually explicit conduct;

c. realistic images representing a minor engaged in sexually explicit conduct.

3. For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

In addition, we reiterate our recommendations in our legal analysis of the Tunisian Press Code concerning criminal sanctions singling out the print media and journalists.

ARTICLE 19 further notes that the availability of pornographic material online has created a large amount of controversy in Tunisia (see section I above). ARTICLE 19 reiterates that pornography is NOT one of the types of expression that must be prohibited under international law. Furthermore, the UN Human Rights Committee recently restated that restrictions on freedom of expression for the protection of public morals must be based on a broad understanding of what 'public morals' means, i.e. one that does not derive exclusively from one social, philosophical or religious tradition.[45]

Nonetheless, we recognise the legitimate concerns of parents to protect their children from access to pornographic content online. This should not, however, come at the expense of freedom of expression, and in particular the right of adults to access such content. For this reason, international organisations such as the Council of Europe have advocated the use of filters under end-users' control in order to strike a proper balance between freedom of expression and the protection of children.[46] By contrast, compulsory content filtering systems imposed by government or a commercial service would not be compatible with international law as it would amount to a form of prior censorship.[47]

Recommendation:

We reiterate the Recommendations contained in our analysis of the Tunisian Press Code: defamation should be decriminalised and the hate speech provisions contained in the Code should be more tightly drafted.

III. Regulation of citizen-journalists and bloggers

ARTICLE 19 is not aware of any particular legal framework regulating citizen journalists and bloggers in Tunisia, which is to be welcomed. Indeed, ARTICLE 19 believes that bloggers should

[45] See UN Human Rights Committee, General Comment No 34., para. 32.

[46] See Recommendation CM/Rec(2008)6 on measures to promote the respect for freedom of expression and information with regard to Internet filters.

[47] See 2011 Joint Declaration cited above at n 28.

not be regulated apart from the same civil and criminal liability laws that apply to others.[48] In particular, bloggers and citizen journalist should not be registered as accredited media organisations. Moreover, they should not be made subject to the same editorial controls as media organisations.

We note that professional journalists expressed their reservations concerning the principle of giving bloggers and citizen-journalists the same guarantees (that professional journalists benefit from) for fear that this could lead to being possibly abused by them, and could be used as a reason for the introduction of new restriction on the freedom of expression.

By contrast, we believe that the definition of journalism should be sufficiently broad so as to encompass bloggers and citizen journalists, and afford them the same rights and legal protection as journalists.

Registration

ARTICLE 19 fully supports the UN Human Rights Committee's definition of journalism outlined above. In our view, journalism is an activity (or function), not a profession. Moreover, it is one that is open to any person to undertake as part of his or her right to freedom of expression, regardless of any particular qualification. We therefore believe that the activities of bloggers and citizen journalists should be protected.

Consistent with this view, and in the same way that we have always distrusted regulation of the print media as a tool for governments to overly restrict the right to freedom of expression and information, we firmly believe that bloggers and citizen journalists should not be subject to any registration requirement.

As already noted above, the UN Human Rights Committee has rejected the view that journalists, including citizen journalist or bloggers, should be registered or licensed. Moreover, the Special Rapporteur has called on States to refrain from adopting real-name registration systems.[49] In other words, they should be allowed to remain anonymous. We fully endorse these views.

Accordingly, we recommend that bloggers and citizen journalists should NOT be required to register or obtain a licence. Similarly, real-name registration policies should be rejected.

Editorial control

ARTICLE 19 believes that bloggers and citizen journalists should NOT be made subject to the same laws of editorial control as journalists. It is well-established under international law that people exercising their freedom of expression have certain 'duties and responsibilities'. However, the scope of such duties and responsibilities must always take account of a person's situation, including their resources and the technical means available to them.[50] For example, it would be unfair to require someone who blogs in their spare time to meet the standards of fact-checking

[48] ARTICLE 19, however, strongly opposes the speech offences contained in the Tunisian Press Code such as criminal defamation. For more details, see our analysis of the Tunisian Press Code, available at: http://www.article19.org/resources.php/resource/2944/en/tunisia:-press-regulation

[49] See n 41 above, ibid., para. 84.

[50] See for example, Stoll v Switzerland, [GC] no.69698/01, para. 102, 10 December 2007. .

and editing that can be reasonably expected from a journalist working for a major media company. The Council of Europe has adopted a similar approach by calling on States to adopt differentiated responses to different level of editorial responsibility. Therefore, ARTICLE 19 recommends that the duties and responsibilities of bloggers and citizen journalists should be limited to the duty of all citizens to respect and obey the law (see section below).

Civil and criminal liability

As already mentioned above, the law does not usually make any distinctions between journalists and the rest of the population for the purposes of civil or criminal liability.[51] Accordingly, bloggers and citizen journalists are not immune to the application of such laws, for example defamation law. However, where they undertake the activity of journalism, they should benefit from the same legal protections as journalists (see below).

Legal protection

ARTICLE 19 believes that citizen journalists and bloggers should be afforded the same legal protections, including the defences of honest opinion, truth, and public interest that are available to media professional organisations in defamation proceedings. Indeed, most civil and criminal defamation laws are expressed in general terms and do not single out journalists as the beneficiaries of such legal protections, although in practice defamation laws may have been applied mainly to statements made by media organisations in the past.

Moreover, given the increasing importance of the Internet as a source for news and information, ARTICLE 19 believes that it would be unrealistic to limit the scope of defences, and legal protections generally, to paid journalists only. This, in our view, also applies to source protection. For this reason, we recently noted in our legal analysis of the Tunisian Press Code that the definition of 'journalist' was too restrictive and that it should include citizen journalists and other individuals engaged in the dissemination of information. We acknowledge, however, that there is currently no consensus at the international level on the availability of source protection to bloggers and citizen journalists.

Recommendations:

- Bloggers and citizen journalists should NOT be specifically regulated;
- Bloggers and citizen journalists should NOT be required to register;
- Bloggers and citizen journalists should NOT be required to register under their real name;
- Bloggers and citizen journalists should NOT be subject to the same duties and responsibilities as journalists;
- Bloggers and citizen journalists should benefit from source protection.

IV. Liability of Internet Service Providers

In Tunisia, the liability of Internet Service Providers (ISPs) is governed by the Decree no.97-501 of 14 March 1997 concerning value-added telecommunications services ('the Telecommunications Decree') and the Regulations of 22 March 1997 concerning the specifications for setting up and operating value-added Internet telecommunications services ('the Internet regulations'), both of which were enacted under the Ben Ali regime. While these laws do

[51] Some provisions of the Tunisian Press Code – which we oppose – are an exception in that they single out 'crimes committed by journalists' or 'through the press.

not appear to have been enforced since the revolution, they remain on the statute book. Furthermore, the decrees of the implementation of the telecommunications code adopted in 2001 and since amended several times, have never been published.

In ARTICLE 19's view, the provisions governing ISP liability in Tunisia are deeply flawed and fail to comply with international standards for the protection of freedom of expression.

Under Article 1 of the Telecommunications Decree, producing, providing access to, disseminating and hosting information by way of electronic services is subject to the Press Code. Article 14 further provides that all ISPs must designate a director responsible for the content that travels across their networks in compliance with the Press Code. Read together, these provisions mean that ISPs are liable for third-party content. The Decree does not provide for any exceptions.

Article 9 of the Internet regulations further expands on the obligations of ISPs in relation to content. In particular, the director responsible for online content is required to constantly monitor content to ensure that no information contrary to public order or good morals remains on the network. Moreover, the director is required to archive hardcopies of content as may be necessary for the purposes of court proceedings and keep such archives for one year. When an ISP closes down or ceases to provide Internet services, the director responsible for online content must turn over all of the ISP's archives to the Tunisian Internet Agency 'without delay'.

In this regard, we welcome the fact that following the revolution, content takedowns have been ordered only by the courts.[52] We also hail the recent decision of the Court of Cassation, which overturned an earlier decision of the Court of Appeal ordering the Tunisian Internet Agency to put in place a filtering and blocking mechanism preventing access to pornographic material.

Nonetheless, we remain concerned that the decision of Court of Cassation failed to establish that blanket filtering or blocking of pornographic material is disproportionate. It should be remembered that any blocking order should comply with the three-part test under international law. In particular, it should have a clear legal basis, pursue a legitimate aim and be proportionate to the aim sought to be pursued. For example, an order to take down a whole website rather a particular webpage would be highly likely to fall foul of international standards for the protection of freedom of expression. As websites may contain both legitimate and illegitimate content, the takedown of a whole website would mean that legitimate content could also be removed, which would be disproportionate. Similarly, there is an inherent risk of overblocking in the mandatory filtering of all pornographic content. Therefore, this type of measure is both disproportionate and in clear breach of international law.

For all these reasons, ARTICLE 19 recommends that the provisions governing ISP liability should be removed immediately. This would also signal Tunisia's commitment to ending state censorship. In addition, the law should reflect the important principle that ISPs, and indeed intermediaries more generally, should only be held liable where they have specifically intervened in particular content. Moreover, they should be required to take down content only upon notice of a court order.

Recommendations:

- Articles 1 and 14 of the Telecommunications Decree which govern ISP liability should be removed;

[52] Ibid.

- Article 9 of the Internet Regulations which lays down the obligations of ISPs in relation to content should be removed;
- The above provisions should be replaced by a new provision granting immunity to intermediaries for third-party content;
- The law should include a provision that intermediaries should be prohibited from monitoring content that travels across their network;
- The law should require that only the courts may grant a blocking/filtering/removal order subject to the principles of necessity and proportionality.

V. Encryption technologies and anonymity

Encrypted technologies

ARTICLE 19 is concerned that Articles 9 and 87 of the Telecommunications decree, Internet Service Providers may only transmit encrypted information subject to the authorisation of the minister of communications and that these sanction all usage of encrypting means by heavy sanctions (including imprisonment) for anybody who uses encrypting means without being authorised. This means that the ability of Internet users to keep their communications private or to use systems to access the Internet and other ICTs without interference and surveillance is severely limited.

The protection of the privacy of communications is essential to creating an environment in which people are confident to express themselves freely. The UN Special Rapporteur on Freedom of Expression has further made it clear that the right to private correspondence gives rise to a comprehensive obligation on the part of the State to ensure that e-mails and other forms of online communication are actually delivered to the desired recipient without interference or inspection by State organs or by third parties.[53]

The blanket ban on the use of encryption technologies without prior approval from the ministry of communication clearly constitutes an arbitrary interference with the right of Internet users to the privacy of their communications. By undermining the confidence of Internet users in the privacy of their communications, it also has a chilling effect on the free flow of information. Accordingly, Article 11 is plainly in breach of both Articles 17 and 19 of the ICCPR.

ARTICLE 19 therefore recommends that these provisions be repealed as well the related regulatory texts (decree N°2001-2727 of 20 November 2011 regarding the conditions and procedures of use of the encrypted technologies, such as that amended by decree N°2007-1070 of 2 May 2007 which establishes the restrictions and sanctions resulting from the use of encrypted technologies). This, however, should not preclude the authorities from seeking a warrant authorising the decryption of communications in carefully defined circumstances under the law, such as the investigation of serious crimes, in the respect of the principles of necessity and proportionality.

Anonymity

ARTICLE 19 is further concerned about Article 8 of the Internet regulations which require ISPs to submit a list of all their subscribers to the public operator, i.e. the Tunisian Internet Authority, on a monthly basis. This requirement is unnecessary and as such impermissible under Article 17 of

[53] See UN Special Rapporteur on Freedom of Expression, cited above at n 41, para.57.

the ICCPR (right to privacy). Moreover, it is likely to lead to self-censorship and as such may be in breach of Article 19 of the ICCPR.

This does not mean that this kind of information should never be made available to the authorities. In particular, the law should define the circumstances in which law enforcement agencies may apply for a warrant authorising the disclosure of the identity of internet users, or as the case maybe, their communications data, or allowing interception of their communications. However, any such measure should be authorised by a judge applying the necessity and proportionality test under international law. Indeed, as Tunisia moves away from the Ben Ali era and its repressive practices, we further suggest the adoption of a new legal framework strictly regulating surveillance along the lines of the internationals standards set out above.

Information security

In addition, Article 19 is concerned by Law N°2004-5 relating to active information security, in that the general nature of this legislation and the extensive power attributed to the national agency of information security (ANSI) are likely to establish a form of censorship of the Internet under the guise of technical responsibilities. It would seem that that this has been the case under the Ben Ali regime.

In fact, this law gives ANSI the mission of controlling public and private information systems, and of supervising the implementation of national strategies on information security. Furthermore, ANSI is in charge of establishing information security technical norms. Yet, the notion of "information security" is not defined in the law nor in the implementing decree. Similarly, neither the law or the implementing decree specifies for what certain filtering software can be used. As the vague nature of the law is a given, we can only conclude that it allows, in theory, the use of filtering techniques such as 'deep packet inspections' for censoring purposes.[54]

ARTICLE 19 also reveals that ANSI is in charge of carrying out obligatory periodic audit of information security of public and private computer networks. In our opinion, this constitutes, in all cases of private networks, an unjustified interference in the right to a private life and freedom of expression, and even more so as ANSI depends directly on the ministry of communication technologies. In this regard, it is noteworthy that in numerous countries, the technical control of private information systems is carried out by the operators providing this type of service, that is to say self-regulation.

In light of the above and regarding surveillance practices under the Ben Ali regime, ARTICLE 19 considers that the risk of the use of law N°2004-5 relative to information security for the purpose of censorship can not be ruled out. This law should at least be reviewed in view of strictly defining the term 'information security' and limiting the rights of ANSI, notably by restricting the area of intervention to a purely technical control of the state's information systems and networks.

Recommendations:

- Articles 9 and 87 of Telecommunications Code and Article 11 of Decree n° 97-501 which bans the use of encryption technologies without prior approval from the authorities should be removed.

- Article 8 of the Decree n° 97-501 which requires ISPs to submit a list of their subscribers to the public operator, i.e. the Tunisian Internet Agency, should be removed.

[54] Deep packet inspection (DPI) allows to analyse the content of packets of data and detect and filter intrusions, or spam or all other type of pre-defined content.

- The need for a review of law N°2004-5 regarding information security with the view of strictly defining the term 'information security' and limiting the rights of the national information security agency regarding the technical control of the state's information systems and networks.

VI. Protection of private life and personal data

Protection of private life

ARTICLE 19 is concerned by the apparent absence of a legal framework governing telephone tapping and access to electronic communication in view of protecting private life in a manner compatible to article 17 of the ICCPR. In this respect, we note that the UN's special rapporteur on the protection and promotion of the freedom of expression recently called the Member States to review their laws relating to the access to communication data in order to align it with international human rights standards applicable in this area.[55] ARTICLE 19 can only reiterate this invitation and encourage the Tunisian government to strictly regulate access to this type of data regarding the right to a private life and to freedom of expression.

Protection of personal data

ARTICLE 19 is concerned about the recent use of law N°2004-63 of 27 July 2004 on the protection of personal data against bloggers. In fact, the Tunisian minister of Foreign Affairs made a complaint against blogger Olfa Riahi, in January 2013. The complaint was lodged based on numerous texts such as articles 89 and 90 of the organic law N°2004-63 concerning the protection of personal data. The blogger in question had raised suspicions about a relationship between the minister and one of his relatives by mentioning that the latter had spent a night in the same hotel as the minister.

According to Article 89 of the law, a person who 'intentionally communicates personal data to make a personal profit or the benefit of another, or by causing the concerned person a loss" is punished by one year in prison and a fine of five thousand dinars. In addition, Article 90 punishes anyone who intentionally deals with personal data without prior notification or authorisation of the national body for the protection of private data, or communicates the personal data without the consent of the concerned people, or the agreement of the official body in the cases planned for by the law.

Yet, the law does not provide exemptions or derogations to the application of provisions of protection of data in the framework of the treatment of data processed for journalistic, artistic, literary or cultural purposes. The derogations are, however, essential to allow journalists, bloggers and citizen-journalists to conduct investigative operations to uncover certain truths.

It is clear from the above that the use, by a blogger, of certain personal data making it possible to identify a person, without having obtained prior authorisation from the national body in this area, makes the blogger immediately punishable according to Articles 89 and 90 of law N°2004-63.

Consequently, the absence of derogations or exemptions to the application of provisions of protection of personal data in the framework of the treatment of data processed for journalistic,

[55] A/HRC/23/40, available at : A/HRC/23/40, http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

artistic, literary or cultural purposes, ARTICLE 19 considers that law N°2004-63 of 27 July 2004 is inconsistent with international law.

Finally, it is worth noting that this law allows different public authorities to process personal data without the consent of the person concerned and without the declaration or authorisation of the national body of the protection of personal data: the extensive powers that the law grants them can push bloggers and citizen-journalists to self-censor for fear of being prosecuted by the authorities, who have all their personal data, for one reason or another.

Recommendations :

- The conditions of access to the content of correspondence and its use by the public authorities should be clearly defined.
- The law on the protection of personal data should be exempt in the application of provision of the protection of data in the framework of processing data processed for journalistic, artistic, literary or cultural purposes.

VII. Access to the Internet and network neutrality

Universal access to the Internet

ARTICLE 19 has already recommended that access to the Internet should be recognised as a right (see section on the Constitution above). In addition, the special mandates for the protection of freedom of expression have suggested policies to foster universal access to the Internet. We therefore encourage the Tunisian Interim Government to pay close attention to these proposals, which are reproduced above.

Licensing of ISPs

As already mentioned above, in Tunisia, Internet services are regulated by the Telecommunications Decree and the Internet regulations, both of which were enacted under the Ben Ali regime.

Under Article 7 of the Telecommunications Decree, ISPs are required to obtain a licence from the Ministry of Communications in order to provide Internet services. Article 7 of the Internet regulations provides that a licence may be obtained subject to a number of technical and financial requirements, type approval of the necessary equipment and a favourable opinion of a commission composed exclusively of government representatives. In addition, ARTICLE 19 understands that ISPs are required to obtain an authorisation from the Tunisian Internet Agency (ATI mentioned above), in order to be able to deliver electronic services.

In ARTICLE 19's view, the current regulatory framework for Internet services falls short of international standards for the protection of freedom of expression. In particular, it clearly emerges from the Telecommunications Decree (501) and the Decree of 14 March 1997 the Internet regulations that the provision of Internet services is under tight government control in violation of those standards.

Under international law, registration of ISPs is not legitimate unless it conforms to the three-part test. In this regard, the UN Special Rapporteur has stated that unlike the broadcasting sector, for which registration or licensing has been necessary to allow States to distribute limited frequencies,

such requirements cannot be justified in the case of the Internet, as it can accommodate an unlimited number of points of entry and an essentially unlimited number of users.[56]

While ARTICLE 19 subscribes to this view, we recognise that limited regulation of the telecommunications sector may be necessary in order to prevent undue state monopoly and ensure equitable access to the Internet backbone infrastructure. In addition, technical registration requirements may be permissible provided that:

(i) there is no discretion to refuse registration once the requisite information has been provided;

(ii) the requirements do not impose substantive obligations on ISPs;

(iii) the requirements are not excessively onerous; and

(iv) the requirements are administered by an independent body.

We note, for example, that in the European Union, the provision of electronic communications networks or services may only be subject to a general authorisation. The company concerned may thus be required to submit a notification but it may not be required to obtain an explicit decision or any other administrative act by the national regulatory authority (NRA) before exercising the rights stemming from the authorisation.[57]

Under current arrangements, by contrast, ISPs are required to obtain a licence directly from the minister of communications, which obviously lacks the independence required under international law. Moreover, the minister enjoys a wide discretion to refuse the grant of a licence, for example if the opinion of the commission made up of government representatives is unfavourable.

Accordingly, we recommend that Decree no.97-501 of 14 March 1997 concerning the regulation of the telecommunications sector should be reviewed to bring it more closely in line with international standards for the protection of freedom of expression. In particular, the provisions requiring ISPs to obtain a licence from the ministry of communications should be abolished in their entirety. Instead, the supervision of compliance with technical requirements should be entrusted to an independent regulator. We stand ready to provide more detailed recommendations regarding the proper legal framework for the regulation of intermediaries. ARTICLE 19 equally recommends accelerating the reform process of the telecommunications sector in the way indicated here-above.

Net neutrality

ARTICLE 19 notes that there is currently no recognition of the net neutrality principle in Tunisia. ARTICLE 19 therefore strongly encourages the Interim Government to espouse this principle along the lines of the Special mandates for the protection of freedom of expression.

---

[56] See UN Special Rapporteur's report cited above at n 41, para. 27. The Special Rapporteur noted, however, that this did not apply to the registration of domain names for purely technical reasons.

[57] For a synopsis of the Authorisation Directive, see:
http://europa.eu/legislation_summaries/information_society/legislative_framework/l24164_en.htm

It should be noted that the Authorisation Directive is part of a 'Telecoms Package' regulating the telecommunications sector in the EU. Further information is available from here:
http://europa.eu/legislation_summaries/information_society/legislative_framework/index_en.htm

Recommendations:

- Article 7 of the Telecommunications Decree (N°97-501 of 14 March 1997) requiring ISPs to obtain a licence from the ministry of communications should be repealed;
- The Telecommunications Decree (501) should be reviewed with a view to establishing an independent regulator for the communications sector;
- The principle of network neutrality should be recognised in the Telecommunications Decree and the Internet Regulations.