ARTICLE 19

Islamic Republic of Iran: Computer Crimes Law

December 2011

Legal analysis

Executive summary

The 2011 Computer Crimes Law of the Islamic Republic of Iran flagrantly violates international human rights law and is an affront to freedom of expression principles. Extensive legal reform, including the repeal of the Computer Crimes Law, is urgently required to protect the right to freedom of expression in Iran.

ARTICLE 19 notes with concern that the Computer Crimes Law of 2011 is only the latest addition to the Islamic Republic of Iran's vast censorship apparatus. It demonstrates the resolve of the Iranian Government to pursue human rights defenders, bloggers and journalists through electronic media: the last available sanctuary for freedom of expression and political dissent in the country.

The Computer Crimes Law is saturated with provisions that criminalise legitimate expression. Crimes against "public morality and chastity" and the "dissemination of lies" are engineered to ensnare all forms of legitimate expression. These include broad criminal defamation and obscenity provisions that are antithetical to the right to freedom of expression. Essential elements of offenses are described with ambiguity and in vague and overbroad terms. No defences are available to individuals acting in the public interest. Unfettered discretion is conferred on the Government to pursue its own prerogatives above the interests of the public and the imperatives of international human rights law.

The Computer Crimes Law mandates severe sentences that penalise legitimate expression and offend the proportionality principal that is fundamental to human rights protection. ARTICLE 19 is particularly appalled at the availability of the death penalty for crimes committed against public morality and chastity. Other sanctions on legitimate expression include lengthy custodial sentences, draconian fines, and judicial orders to close organisations and ban individuals from using electronic communications. These penalties also apply to Internet Service Providers that fail to enforce content-based restrictions, incentivising the private sector to promulgate Iran's censorship culture.

ARTICLE 19 believes that restoring the right to freedom of expression in Iran requires wholesale reform to redress the conceptual failure signified by the Computer Crimes Law. Protection and promotion of freedom of expression must be reasserted as norms and limitations on free expression as the exception.

Recommendations

1. The Iranian Government must repeal the Computer Crimes Law in its entirety.
2. Comprehensive legal reform must include amending the Iranian Constitution to safeguard freedom of expression and the repeal of provisions of the 1986 Press Law and Islamic Penal Code that restrict the legitimate exercise of this right.
3. Iran must immediately abolish the death penalty and decline to impose custodial sentences for expression-related offenses, except of those permitted by international legal standards and with adequate safeguards against abuse.
4. Iran must repeal any law that imposes liability on Internet Service Providers for the content of expression that passes through their systems.
5. Iran must immediately release all who are imprisoned, detained and prosecuted for the legitimate exercise of their right to freedom of expression.

Table of Contents

About the Article 19 Law Programme

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, or if you have a matter you would like to bring to the attention of the ARTICLE 19 Law Programme, you can contact us by e-mail at legal@article19.org. For more information about this analysis and about the work of the Iran project of ARTICLE 19, please contact Amir Bayani, Iran Programme Officer at amir@article19.org or visit Azad Tribune: http://www.article19.org/pages/en/azad-tribune.html.

Introduction

In this analysis, ARTICLE 19 details its concerns regarding the Computer Crimes Law adopted by the Islamic Republic of Iran (Iran) in January 2010. The analysis outlines Iran's obligations under international human rights law, in particular the right to freedom of expression and freedom of information under the International Covenant on Civil and Political Rights (ICCPR). The analysis then details the domestic legal framework. Ultimately it reviews the Computer Crimes Law for compliance with Iran's international freedom of expression obligations and makes recommendations to bring Iran into compliance with respective international standards.

Two recent advancements in respect of freedom of expression and the Internet inform this analysis: the June 2011 International Special Rapporteurs of Freedom of Expression Joint Declaration on Freedom of Expression and the Internet, and the June 2011 United Nations Human Rights Committee (HR Committee) General Comment No.34. Both elucidate the application of freedom of expression principles to electronic and Internet-based modes of communications, providing contemporary and authoritative guidance on Iran's violations of fundamental principles of international human rights law.

This analysis builds upon ARTICLE 19's extensive experience raising awareness of Iran's censorship structures and supporting Iran's civil society in eluding state control and suppression. To this end ARTICLE 19 established Azad Tribune, an online platform for bloggers, journalists and activists to discuss issues relating to freedom of expression and freedom of information in Farsi and English.[1] ARTICLE 19 regularly advocates on behalf of bloggers, journalists and activists in Iran. In 2009, ARTICLE 19 raised its concerns about Internet censorship as well as the prosecution of bloggers and cyber-activists in the submission to the Human Rights Council in preparation for the universal periodic review of Iran.[2] Most recently in 2011, ARTICLE 19 has called for the release of Mahnaz Mohammadi and Pegah Ahangarani, renowned film-makers and prominent human rights defenders incarcerated because of their political views.[3] It is because of brave individuals like these that Iran has been unable to hide its repressive activities.

Reflecting global trends, the Internet has become the locus of political debate and activism within Iran. The Internet is widely credited with uniting and empowering previously fractured groups of repressed individuals to demand greater accountability and transparency in their societies. Cognisant of this, the Iranian Government has monopolised control over the Internet, developing a sophisticated filtration system, blocking content and employing a specialist web crime task force to target online activists.

ARTICLE 19 is concerned that the Computer Crimes Law provides the Iranian Government with yet another instrument with which to harass, intimidate, and detain those that dare to criticise it. The Computer Crimes Law's ambiguity, coupled with the severity of its sentences and its disregard for the importance of freedom of expression in enabling protection of other human rights renders it irretrievably flawed. ARTICLE 19 urges the Government of the Islamic Republic of Iran to immediately repeal the Computer Crimes Law and to enact legislation safeguarding the right to freedom of expression and access to information. At the same time, all those who are prosecuted or have been convicted for exercising their right to freedom of expression should be immediately acquitted.

---

[1] ARTICLE 19 press release http://www.azadtribune.org/en/content/press-release.

[2] ARTICLE 19's submission to the universal periodic review of Iran is available at: http://www.article19.org/data/files/pdfs/submissions/iran-article-19-submission-to-the-un-universal-periodic-review.pdf

[3] See Iran: Free unjustly detained women film-makers; available at http://www.article19.org/resources.php/resource/2260/en/iran:-free-unjustly-detained-women-film-makers.

International freedom of expression standards

Freedom of expression and information is a fundamental human right. The full enjoyment of this right is central to achieving individual freedoms and to developing democracy, as demonstrated by the ongoing democratic transitions occurring in several of Iran's near neighbours. Freedom of expression is a necessary condition for the realisation of the principles of transparency and accountability that are, in turn, essential for the promotion and protection of all human rights.

The Computer Crimes Law in Iran engages a number of international freedom of expression standards that form the basis of the legal analysis below. This section identifies those international human rights provisions most relevant to the protection of freedom of expression and in particular their relationship to the penal regulation of computer use.

Universal Declaration of Human Rights

Article 19 of the Universal Declaration of Human Rights (UDHR)[4] 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.[5]

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.[6] Article 19 of the ICCPR guarantees the right to freedom of expression as follows:

> 1. Everyone shall have the right to freedom of opinion
> 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art or through any other media of his choice.

Iran signed the ICCPR on 4 April 1968 and ratified it on 24 June 1975. Iran is therefore legally bound to respect and to ensure the right to freedom of expression as contained in Article 19.

On 21 June 2011, the HR Committee, as treaty monitoring body for the ICCPR, issued General Comment No.34 in relation to Article 19.[7] 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 and detailed elucidation of international law related to

---

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

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

[6] 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).

[7] Human Rights Committee, General Comment No. 34, Article 19: Freedoms of opinion and expression, adopted at 102nd session, Geneva, 11-29 July 2011; available at http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf.

freedom of expression and access to information.[8] It is contemporary to and instructive on a number of freedom of expression concerns raised by the Computer Crimes Law.

Importantly, General Comment No.34 affirms that Article 19 of the ICCPR protects all forms of expression and the means of their dissemination, including all forms of electronic and internet-based modes of expression.[9] States party to the ICCPR are required to take account of the extent to which developments in information technology have substantially changed communication practices around the world. General Comment No.34 calls on States parties to take all necessary steps to foster the independence of these new media and to ensure access of individuals thereto.[10] This includes an obligation to "proactively put in the public domain Governmental information of public interest …(and)… make every effort to ensure easy, prompt, effective and practical access to such information."[11] Default recourse to secrecy without individually assessing the public interest of that information therefore violates Article 19 of the ICCPR.

As a state party to the ICCPR, Iran must ensure that any of its laws attempting to criminalise or otherwise regulate electronic and internet-based modes of expression, including accessing and disseminating information, comply with Article 19 of the ICCPR.

Limitations on the Right to Freedom of Expression

While the right to freedom of expression is a fundamental right, it is not guaranteed in absolute terms. Article 19(3) permits the right to be restricted in the following respects:

> 3. 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 prescribed 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) prescribed by law, ii) pursue a legitimate aim; and iii) that they conform to the strict tests of necessity and proportionality.[12]

General Comment No.34 states that restrictions on internet-based, electronic or other such information dissemination systems are only permissible to the extent that they are compatible with Article 19 paragraph 3.[13] This includes restrictions on Internet service providers.

i) "Provided by law"

Article 19(3) requires that restrictions on the right to freedom of expression must be prescribed by law. This requires a normative assessment; to be characterised as a law a norm must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly.[14] Ambiguous or

---

[8] ARTICLE 19 statement on HR Committee Comment No.34, 5 August 2011; available at http://www.article19.org/resources.php/resource/2631/en/un:-article-19-welcomes-general-comment-on-freedom-of-expression.

[9] Paragraph 12, HR Committee General Comment No.34

[10] Paragraph 15, HR Committee General Comment No.34

[11] Paragraph 19, HR Committee General Comment No.34

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

[13] Paragraph 43, HR Committee General Comment No.34

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

overly broad restrictions on freedom of expression deficient in elucidating the exact scope of their application are therefore impermissible under Article 19(3).

General Comment No.34 further provides that for the purpose of Article 19(3) a law may not confer unfettered discretion for restricting freedom of expression on those charged with executing that law.[15] Laws must provide sufficient guidance to those charged with their execution to enable them to ascertain what sorts of expression are properly restricted and what sorts are not. The requirement that the law be sufficiently precise for this purpose is closely related to the requirements of necessity and proportionality. It ensures that restrictions on freedom of expression are only employed for legitimate protective objectives and limits the opportunity to manipulate those restrictions for other purposes.

ii) "Legitimate aim"

Interferences with the right to freedom of expression must pursue a legitimate protective aim as exhaustively enumerated in Article 19(3)(a) and (b) ICCPR. Legitimate aims are those that protect the human rights of others, protect national security or public order, or protect public health and morals. As such, it would be impermissible to prohibit information dissemination systems from publishing material solely on the basis that they cast a critical view of the government or the political social system espoused by the government.[16] Nor would it be permissible to achieve such illegitimate objectives through a reliance on Article 19(3) that is merely pre-textual. Narrow tailoring requires that permissible restrictions be content-specific: it would be impermissible to close a website or liquidate an ISP when it is possible to achieve a protective objective by isolating and removing the offending content. Where a State does limit freedom of expression, the burden is on that state to show a direct or immediate connection between that expression and the legitimate ground for restriction.

The Johannesburg Principles on National Security, Freedom of Expression and Access to Information[17] (Johannesburg Principles), a set of international standards developed by ARTICLE 19 and international freedom of expression experts, are instructive on restrictions on freedom of expression that seek to protect national security. Principle 2 of the Johannesburg Principles states that restrictions sought to be justified on the ground of national security are illegitimate unless their genuine purpose and demonstrable effect is to protect the country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force. The restriction 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. Principle 15 states that a person may not be punished on national security grounds for disclosure of information if (1) the disclosure does not actually harm and is not likely to harm a legitimate national security interest, or (2) the public interest in knowing the information outweighs the harm from disclosure.

General Comment No.34 also notes that extreme care must be taken in crafting and applying laws that purport to restrict expression to protect national security. Whether characterised as treason laws, official secrets laws or sedition laws they must conform to the strict requirements of Article 19(3). General Comment No.34 provides further guidance on laws that restrict expression with the purported purpose of protecting morals. Such purposes must be based on principles not deriving exclusively from a single tradition but must be understood in the light of the universality of human rights and the principle of non-discrimination.[18] It would therefore be incompatible with the ICCPR, for example, to privilege one particular religious view or historical perspective.

---

[15] *Ibid.*

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

[17] Adopted on 1 October 1995. These Principles have been endorsed by the UN Special Rapporteur on Freedom of Opinion and Expression and have been referred to by the United Nations Commission on Human Rights in each of their annual resolutions on freedom of expression since 1996.

[18] Paragraph 32 HR Committee General Comment 34.

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 requires that a restriction on expression is not over-broad and that it is appropriate to achieve its protective function. It must be shown that the restriction is specific and individual to attaining that protective outcome and is no more intrusive than other instruments capable of achieving the same limited result. General Comment No.34 states that generic bans on the operation of certain websites and systems are never proportionate and are therefore incompatible with Article 19(3).

Joint Declaration on Freedom of Expression and the Internet

In June 2011, the four International Special Rapporteurs on Freedom of Expression[19] issued a Joint Declaration on Freedom of Expression and the Internet (Joint Declaration) in consultation with ARTICLE 19. The four International Rapporteurs represent the Americas, Europe, Africa and the United Nations.[20] In paragraph 1(a) the Joint Declaration affirms the application of freedom of expression rights to the Internet. Paragraph 4(b) of the Joint Declaration emphasises that the imposition of criminal liability for expression-related offenses must take into account the overall public interest in protecting both expression and the forum in which it is made.

Cyber Security and Respect for Human Rights

International resolutions and instruments on cyber security recognise the importance of balancing security imperatives with fundamental human rights, in particular the right to freedom of expression. The UN General Assembly Resolution on the "Creation of a global culture of cyber security"[21] states that "security should be implemented in a manner consistent with the values recognised by democratic societies, including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency."

From a comparative perspective, ARTICLE 19 also notes that the preamble to the Council of Europe Convention on Cybercrime (2001) states that parties must be "mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights ... which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy."[22] It is noteworthy that the Convention contains no content-based restrictions other than those relating to child pornography. The potential for domestic Cybercrimes laws to target political dissent is recognised in the Convention at Article 27(4)(a), which allows states to refuse assistance to other states party if that request is perceived to relate to a politically motivated prosecution. With 32 states party, the convention has the largest membership of any international legal instrument on this topic. While Iran is not a signatory, the

---

[19] The United Nations Special Rapporteur on Freedom of Opinion and Expression, Frank LaRue; the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights of the Organization of American States, Catalina Botero Marino; the Organization for Security and Cooperation in Europe Representative on Freedom of the Media, Dunja Mijatoviæ; and the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression, Faith Pansy Tlakula

[20] Joint Declaration on Freedom of Expression and the Internet, 1 June 2011; available at http://www.article19.org/data/files/pdfs/press/international-mechanisms-for-promoting-freedom-of-expression.pdf.

[21] See Resolution adopted by the General Assembly, *on the report of the Second Committee (A/57/529/Add.3)*, 57/239, A/RES/57/239, 31 January 2003; available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf.

[22] Convention on Cybercrime, adopted in Budapest, 23.XI.2001; available at http://conventions.coe.int/Treaty/en/Treaties/html/185.htm.

Convention provides a model for a cyber crimes law that complies with international human rights standards.[23]

UN General Assembly Resolution on the Situation of Human Rights in Iran

In November 2009, the UN General Assembly passed the Resolution on the Situation of Human Rights in Iran[24] with 74 Member States voting in favour and 48 Member States voting against. The Resolution calls upon Iran to address its human rights situation, in particular relating to freedom of expression and the harassment of human rights defenders. UN General Assembly Resolutions have moral and political force but do not have binding legal effect.

The Resolution states that Iran's abuse of freedom of opinion and expression rights is ongoing, systemic and serious. The media, Internet users and trade unions are identified as targets of this repression.[25] The signatories also pointed to the disruption of telecommunications and Internet technology as a means of disrupting freedom of expression and association. It is noted that repression is often gendered, targeted disproportionately at women and girl human rights defenders.[26]

The Resolution calls for an end to the harassment, intimidation and persecution of political opponents and human rights defenders, students, academics, journalists, other media representatives, bloggers, clerics and lawyers. It calls for the release of persons imprisoned arbitrarily or on the basis of their political views and those detained following the Presidential election of 12 June 2009.

[23] *Ibid.*

[24] United Nations A/C.3/64/L.37

[25] Situation of human rights in the Islamic Republic of Iran, 29 October 2009, 2f UN A/C.3/64/L.37; available at http://news.bahai.org/sites/news.bahai.org/files/documentlibrary/iu_UN_Resolution_Nov_2009.pdf.

[26] *Ibid.*

Domestic legal framework

This section provides a brief overview of the domestic legal framework that the Computer Crimes Law exists within and the greater censorship apparatus that it forms a part of.

The censorship of electronic and Internet-based expression in Iran predates the enactment of the Computer Crimes Law in 2011. Provisions of the Constitution of the Islamic Republic of Iran, the Press Law of 1986 and the Islamic Penal Code provide for content-based restrictions on freedom of expression and have been the principal instruments of repressing electronic and Internet-based expression.

The Computer Crimes Law is merely an addition to this censorship apparatus. The law replicates many content-based restrictions found elsewhere in Iran's legal framework but targets them specifically at the use of technology. Reforming or repealing this legislation in isolation still leaves available the option of reverting to alternative tools of repression. It is important to recognise that addressing the deficiencies of the Computer Crimes Law can only lead to the realisation of the right to freedom of expression as part of a much broader reform agenda in Iran.

Constitution of the Islamic Republic of Iran

The Constitution of the Islamic Republic of Iran entrenches over-broad qualifications on the right to freedom of expression. Article 24 provides that "publications and the press have freedom of expression, except when it is detrimental to the fundamental principles of Islam or the rights of the public." Fundamental principles of Islam are not defined and rights of the public are not enumerated. The pre-amble to the Constitution reflects this inner conflict. It provides that the media should be used as a "forum for healthy encounter of different ideas, but they must strictly refrain from diffusion of destructive and anti-Islamic practices."

The Constitution lays the foundations for the institutionalisation of censorship. A public interest in censorship is recognized but the public interest in freedom of expression and information disclosure is not. Discrimination and arbitrariness are simultaneously encouraged by privileging one religious belief system while failing to define it. Unlike Article 19(3) ICCPR, the Constitution does not ensure narrow tailoring to prevent the subversion of exceptions into norms. A combination of internal-contradictions and deliberate ambiguities grant lawmakers and law enforcement almost absolute discretion in regulating expression and the channels for it.

Press Law of 1986

The Press Law of 1986, as amended in 2000, extends broad content-based restrictions from the traditional media to electronic and Internet-based modes of expression. Although the amendment requires that electronic publications seek licenses to fall within the scope of the Law, this has proven impracticable and the Iranian Government has asserted that the Press Law applies to all internet-based publications irrespective of the license requirement.[27]

Although the law contains guarantees against censure and government control,[28] it limits the role of the press to "constructive criticism"[29] based on "logic and reason and void of insult, humiliation and detrimental effects."[30] Reports may only be published in pursuit of one of five "legitimate objectives" including "to campaign against manifestations of imperialistic culture…and to propagate and promote

[27] Open Net Initiative 2009 Report on Iran, at Note 35.

[28] The Press Law 1986, Article 4.

[29] The Press Law 1986, Article 3.

[30] The Press Law 1986, Article 3, Note 1.

genuine Islamic culture and sound ethical principles."[31] Again, these normative objectives are ambiguous are therefore vulnerable to manipulation by law enforcement authorities.

The Press Law prohibits publishing on a broad range of matters including those related to atheism, encouraging dissent against the security, dignity or interests of the State, publishing sensitive information without prior authorization, insulting Islam or offending State and religious officials, any libel, or quoting articles from the deviant press or parties opposed to Islam in such a manner as to propagate those ideas.[32] Key terms within the Press Law are not defined, granting indeterminable scope to broad-content based restrictions that purport to serve no legitimate Article 19(3) ICCPR interest. The Press Law of 1986 has institutionalised and preserved censorship of legitimate expression in violation of international human rights standards.

Islamic Penal Code

The Penal Code of Iran contains a range of restrictions on expression that apply as the general law alternative to the Press Law of 1986. Authorities have tended towards use of the Penal Code rather than the Press Law because it does not require open trials in the presence of the jury.[33]

The Penal Code contains a range of expression-related offenses that carry excessive penalties. These include capital punishment or up to five years imprisonment for insulting religion,[34] up to seventy-four lashes or two years imprisonment for creating anxiety and unease in the public's mind, spreading false rumours, or writing about acts which are not true.[35] The Penal Code also criminalises insulting the Supreme Leader,[36] insulting any of the leaders of the three branches of government,[37] and satirising another person.[38]

The Computer Crimes Law replicates many of these content-based penal provisions so that their application to electronic and Internet-based communications is beyond doubt.

Background to the Computer Crimes Law

The enactment of the Computer Crimes Law is the latest development in the Iranian Government's struggle to monopolise control over Internet access and repress Internet-based expression. The Iranian Government has developed a centralised system for Internet filtering, created institutions tasked with monitoring and censoring Internet-use and engaged the Revolutionary Guard in enforcing Internet content standards.

In 2002, the Committee Responsible for Determining Unauthorised Sites was established to identify unauthorised websites and to block specific domains without recourse to the judiciary.[39] The implementation of filtering decisions has been centralised in the Technology Company of Iran, an agency of the Ministry of Information and Communication Technology. Through these mechanisms, accompanied by specific judicial orders, websites critical of the regime are frequently blocked.

---

[31] The Press Law 1986, Article 2(d).

[32] The Press Law 1986, Article 6.

[33] Open Net Initiative 2009 Report on Iran, at Note 44.

[34] Islamic Penal Code, Article 513.

[35] Islamic Penal Code, Article 698.

[36] Islamic Penal Code, Article 515.

[37] Islamic Penal Code, Article 514.

[38] Islamic Penal Code, Article 700.

[39] Iran's CSOS Training and Research Center, A Report on the Status of the Internet in Iran (2005).

Following widespread protests in 2009, a new web crime task force was established to reinforce censorship and fight cyber crime. The creation of this web crime task force preceded the establishment of a computer crimes penal code by almost two years. In this time, it is likely that the task force has developed its own preferred methods of censorship without the guidance of law. The Computer Crimes Law provides little limitation on the powers of the task force, instead granting law enforcement authorities a more explicit mandate to regulate electronic and Internet-based expression.

Analysis of the Computer Crimes Law

The Computer Crimes Law[40] is made up of 56 articles divided into 3 parts: Part One, Crimes and Punishment; Part Two, Civil Procedure; Part Three, Other Regulations. No article in the legislation indicates the overarching purpose of the law, nor provides for definitions of key terms. A handful of generally inadequate definitions are provided for with sporadic specificity in footnotes to a minority of articles. The law contains no guarantee for the right to freedom of expression or access to information.

At the outset, ARTICLE 19 notes that the Computer Crimes Law contains no definitions of key terms used throughout the law. For example, the terms "illegal access", "access", "confidential data", "disruption", "interception" and the like. This lack of definitions and vagueness in terminology is problematic, since they can be interpreted in various ways. Furthermore, the Cyber Crime Law does not specify whether the crimes enumerated in the law have to be committed intentionally (or at least with dishonest intent) or whether also unintentional or negligent offences warranty the same penalties.

This section analyses the most problematic provisions of the Cyber Crime Law in greater detail and points out discrepancies between the Law and the international freedom of expression standards outlined above.

Part One: Crimes and Punishment

Chapter One – Crimes against Privacy of Data, Computer and Telecommunication Systems

Article 1 criminalizes "illegal access" to data, computers and telecommunication systems that are protected by "security measures."

Despite of the title of Chapter One, the Farsi wording of Article 1 indicates that these provisions apply solely to "data, computers and telecommunications systems" of the government and not to those of individuals or non-state bodies. The term "security measures" is not explained in Article 1 or in any other section of the Law. Article 1 does not detail the essential elements that would require proof for a conviction.

ARTICLE 19 believes that the provisions of Article 1 may be manipulated to target individuals in possession of information the government would rather suppress, as it may be alleged that the information was attained by a breach of security measures.

Restrictions on access to information can only be justified if they strictly conform to the three-part test contained in Article 19(3) ICCPR. The measure must be prescribed by law, pursue a legitimate interest, and be proportionate and necessary.

Article 1 is not "prescribed by law" because it is not formulated with sufficient precision to enable an individual to regulate his or her conduct according to its terms. Article 1 fails to define any of its key terms, including "illegal access", nor the nature of the interest the law seeks to protect. There is no requisite mental state for finding culpability, nor a requirement that harm be shown. This ambiguity allows law-enforcement officers significant discretion to manipulate the law and apply it against people who have not knowingly or intentionally committed a crime.

[40] The text of the Cyber Crime Law is available upon the request from ARTICLE 19.

The offense is not narrowly tailored to protect a legitimate interest. The title to Chapter One suggests that Article 1 protects privacy interests, a "right of others" protected by Article 19(3)(a) of the ICCPR and Article 17 of the ICCPR. However, the ICCPR does not confer a human right to privacy on the government. In contrast, Article 19 of the ICCPR imposes a positive obligation on the government to disclose information that is in the public interest. The Government may only invoke Article 17 of the ICCPR to deny access to such information where it is absolutely necessary to protect natural persons' privacy rights under Article 19(3)(a) of the ICCPR. As a legitimate government interest is not engaged, the measure cannot be said to be a necessary or proportionate means of achieving that end. Even if such a legitimate aim were engaged, the restriction fails to demonstrate a direct and immediate connection between the restricted expression and the harm prevented. It could not, therefore, be said to be necessary or proportionate.

Article 1 provides for the imposition of custodial sentences of 91 days up to 1 year and/or a fine of a minimum 5 million Rials (€327) up to a maximum of 20 million Rials (€1308). Minimum sentences are equivalent to mandatory sentences. These excessive penalties further violate the proportionality requirement. The sentencing judge must have the power to adjust sentences according to the nature of the information accessed and the harm caused.

Article 2 of the Cyber Crime Law, under the heading of "Illegal Spying", criminalises gaining illegal access to content being transmitted through "non-public" communications by computer, telecommunication, electromagnetic or optical systems.

Article 2 prevents any person without governmental authority from intercepting communications between private or public individuals. Again, the key provisions are not defined, including "illegal access", "content", "transmitted" and "private communications". The requisite mental state for the offense is not elicited, allowing an individual to face penal sanctions without knowingly committing the act in question nor intending any particular result. Law enforcement authorities could exploit this ambiguity to arbitrarily target human rights defenders legitimately engaged in public information gathering. It is foreseeable that individuals who publicise information related to government wrongdoing could be accused of gaining their information by "illegal spying." Exploiting Article 2 to suppress such criticism would be a violation of Article 19 ICCPR.

Moreover, ARTICLE 19 is concerned that Article 2 does not protect private and public individuals from unlawful interceptions carried out by the government. We note that Article 17 of the ICCPR binds states to refrain from arbitrary or unlawful interferences with individuals' privacy rights. The protection of communications is essential to creating an environment in which people are confident in their autonomy to determine which ideas they share, when they share them and with whom they share them. This sense of security is fundamental to the functioning of developing and established democracies. The HR Committee has held that interceptions of private communications by Governments must be provided for by law, be in accordance with the provisions, aims and objectives of the Covenant and be reasonable in the particular circumstances of the case.[41] It would therefore be unlawful to employ surveillance and interception techniques to infringe on individual's freedom of expression rights as guaranteed by Article 19 of the ICCPR.

This concern is even more acute as ARTICLE 19 is aware that the Iranian Government systematically monitors and intercepts the communications of people within its jurisdiction, in violation of Article 17 of the ICCPR and Article 19 of the ICCPR. For Iran this is necessary to enforce broad content-based restrictions on expression (see Chapters 4 and 5). To fully comply with its obligations under the ICCPR, Iran must clarify the particulars of Article 2 and specify the limited circumstances in which public authorities can lawfully intercept communications with safeguards to prevent abuse.

[41] *Antonius Cornelis Van Hulst v. Netherlands*, Communication No 903/1999 (at paragraph 7.3).

Article 2 provides for minimum custodial sentences and fines. Minimum sentences do not provide the sentencing judge with the discretion to modify sentences to proportionately reflect the nature of the offense, the harms caused and any mitigating factors.

Article 3 of the Cyber Crime Law, under the heading of "Computer Espionage", broadly criminalises access to and the sharing of "confidential" governmental information. Three degrees of the offense share the common principal act of "illegal access to confidential data, transmitted or saved, on computer and telecommunication systems." Subparagraphs (a) provides principal liability for anyone who accesses or obtains confidential data, or spying on confidential content being transmitted. Subparagraphs (b) and (c) provide liability for individuals who make confidential data available to unauthorised individuals or foreign governments, organisations, companies or groups.

Like previous articles, Article 3 of the Cyber Crime Law does not possess the qualities of accessibility or certainty to be considered "prescribed by law" under Article 19(3) of the ICCPR. It again fails to define what the Computer Crimes Law means by "illegal access." The definition provided for "confidential data" is particularly problematic. Note 1 makes a provisional suggestion that it is information that when disclosed damages the security or interests of the country. Note 2 acknowledges that this definition is insufficient and confers on the Ministry of Intelligence, in collaboration with other ministries and the military, the power to define, identify, classify and protect "confidential data." ARTICLE 19 has not been able to gain access to this guidance. This delegation of legislative authority to the executive concentrates power in that arm of government and allows it to penalise conduct based on its own prerogatives. We note that the HR Committee's General Comment No.34 explicitly provides that a law must not confer unfettered discretion for limiting freedom of expression on those charged with executing the law.[42]Significant clarification of this provision is required before it can be considered "prescribed by law" under Article 19(3) ICCPR.

A restriction on free expression must pursue a protective aim as contained in Article 19(3) of the ICCPR. Article 19(3)(b) permits restrictions on freedom of expression that safeguard national security or public order. Article 3 is illegitimate as it claims to protect two values that are much more generic: "security" and "interests of the country." Even national security interests may only justify restrictions on expression in certain narrow circumstances. Johannesburg Principle 2 states that restrictions sought to be justified on this basis are illegitimate unless their genuine purpose and demonstrable effect is to protect the country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force. Article 3's reliance on the broader "security" or "interests of the country" indicates that the provision may be targeted to insulate the government from criticism. Such a pre-textual reliance on "national security" interests to suppress legitimate speech would directly contravene Article 19 of the ICCPR.

Further, restrictions under Article 19 of the ICCPR must be necessary and proportionate. However, Article 3 of the Cyber Crime Law does not provide the least restrictive means available to safeguard national security. The provision fails to demonstrate a direct and immediate connection between the expression and the harm sought to be prevented. Johannesburg Principle 15(1) states that individuals must not be punished for conduct unless actual or likely harm to national security flows from the prohibited act. The broad definition of "confidential data" allows the punishment of information disclosure that does not and is not likely to harm national security interests.

Article 3 also fails to ensure that interests in national security are properly balanced against the interest in protecting legitimate expression. Johannesburg Principle 15(2) states that legal defences must safeguard disclosures of information where the public interest of that act outweighs the potential harm caused to national security. Article 3 does not provide such a defence. Human rights defenders, journalists, and bloggers acting as "whistleblowers" to expose wrongdoing through the release of information the government would rather suppress are therefore vulnerable under this law. In addition,

[42] *Supra note* 12.

Johannesburg Principle 17 requires that where confidential information is already disclosed, any justification for trying to stop further publication will be overridden by the public's right to know. Article 3 does not meet these standards. On the contrary, Article 3 preserves the harshest penalties for acts that arguably would carry the greatest public interest: disclosing information on government misconduct to organisations like the United Nations and foreign human rights organisations. Article 3 must provide explicit public interest defences to protect whistleblowers and those who publish information already in the public domain.

Severe custodial sentences apply to Article 3. Provisions (b) and (c) provide for minimum custodial sentences of between two and five years respectively, with maximums set at ten and fifteen years. Only provision (a) restricts punishment to the imposition of fines. These sentences are far in excess of what would be proportionate for much of the conduct feasibly within the scope of these prohibitions. Minimum sentences do not provide the judge with the discretion to modify sentences to proportionately reflect the nature of the offense, the harms caused and any mitigating factors.

Article 4 of the Cyber Crime Law, under the heading Computer Espionage, criminalises breaching security measures with the intention of accessing confidential data on computers and telecommunication systems. This essentially covers unsuccessful or incomplete attempts at committing an Article 3(a) offense.

Article 4 shares with Article 3 a failure to define its key terms. The concept of confidential data remains as broad and malleable. Again the provision purports to safeguard the two vague values of "security" and "interests of the country." The analysis contained in Article 3 on the scope of "confidential data" and the illegitimacy of an attempted Article 19(3)(b) ICCPR national security justification for these restrictions applies to Article 4 also.

Although the sentences imposed are less severe than in Article 3, Article 4 may offend Johannesburg Principle (15)(1) more on the basis that it imposes criminal sentences on attempts, where the likelihood of harm is even more remote.

Article 5 of the Cyber Crime Law imposes personal criminal liability on government officials trained and appointed accountable for the protection of confidential data for acts equivalent to those detailed in Article 3 (b) and (c).

Article 5 imposes liability only in relation to confidential data as defined in Article 3, Notes 1 and 2. The scope of the term is therefore as ambiguous and wholly inadequate in this provision as it is in Article 3. This provision differs from Article 3 (b) and (c) in its specification of a requisite mental state for the offense. However, the standard of fault is very low. Criminal penalties may be imposed for negligent acts that are not necessarily committed knowingly or intentionally. Imposing severe criminal penalties for minor degrees of fault is disproportionate to the nature of the act.

Article 5 also fails to provide for a public interest defence where the value of the disclosure outweighs the harm to national security. Johannesburg Principle 16 provides that no person may be subjected to any detriment on national security grounds for disclosing information that he or she learned by virtue of government service if the public interest in knowing the information outweighs the harm from disclosure. Without a public interest defence to protect legitimate acts of whistleblowers Article 5 violates Article 19 of the ICCPR.

Chapter Two – Crimes against Authenticity and Integrity of Data, Computer and Telecommunication Systems

Article 6 of the Cyber Crime Law contains two offenses that carry the label of "fraud" without requiring proof of intending or causing deceit. Article 6a relates to "reliable" data while 6b relates to all data and existing marks on memory cards, central processing units, and chips of computers or telecommunication systems.

The distinction between reliable data and other data is not detailed in the Cyber Crime Law. Similarly, the acts of "alteration" and "falsification" are not defined. The obscurity of Article 6 makes assessing its impact on the right to freedom of expression particularly difficult. It may simply apply to prevent government records and systems from being tampered with, but it may be broadly interpreted to achieve less legitimate ends. The law must be reviewed and redrafted so that the conduct it prohibits is clear. In its current state ARTICLE 19 is unable to provide a more detailed legal analysis of its implications for freedom of expression.

Article 7 of the Cyber Crime Law extends liability to those who knowingly use data altered or falsified as described in Article 6. Again the purpose of this provision is unclear. The clarity of this article will rest on adequate amendments being made to Article 6, particularly the meanings of "altered" and "falsified" and the interests these provisions seek to protect. In its current form the law is too ambiguous to determine whether or not it engages the right to freedom of expression.

Article 9 of the Cyber Crime Law criminalises the entering, transferring, distributing, deleting, deterring, manipulating or corrupting of data, electromagnetic waves or optical fibres of another's computer or telecommunication systems or damaging their operation.

Article 9 is drafted in such broad terms that it could feasibly cover any use of a computer belonging to another. The title to the chapter suggests that the provision is aimed at protecting against the "corruption and damage" of data, computer and telecommunication systems. This provides little guidance on the purpose of this prohibition, the mental state of an individual committing the offense, or the nature of the "corruption" or "damage" caused. ARTICLE 19 recommends that the purpose of this provision is reviewed and that it is redrafted with greater specificity in light of the analysis provided in this brief as a whole. In its current form it does not appear to have the minimal quality of law that would be required to provide a legal analysis of it.

Article 10 of the Cyber Crime Law criminalises "concealing data, changing passwords, and/or encoding data that could deny access of authorised individuals to data, computer and telecommunication systems."

Article 10 potentially criminalises the encryption of Internet communications that evades government surveillance and the possibility of detection for expression-related offenses. Encryption effectively denies authorised individuals that monitor government-controlled proxy-servers access to the encrypted content. Article 10 may allow individuals to be prosecuted for the act of encryption alone without investigation of the unencrypted content for prosecution under other laws. This raises particular concerns for human rights defenders, journalists and bloggers that have had to resort to these techniques due to effectively communicate. Criminalising encryption would therefore have a broad chilling effect on legitimate expression. The restriction must consequently be scrutinised under the three-part test of Article 19(3) of the ICCPR.

Article 10 is not formulated with sufficient clarity to be prescribed by law. The essential elements of the offense are not defined and there is no requisite mental state for the imposition of criminal liability.

Liability may also be imposed without a need to show that the concealment or encoding of data caused harm.

Moreover, ARTICLE 19 notes that the provisions of Article 10 of the Cyber Crime Law does not purport to pursue any of the legitimate aims contained in Article 19(3) of the ICCPR. The ICCPR does not permit Governments to prescribe the manner in which people communicate or grant them a generic entitlement to access data held by individuals. Rather, Article 17 of the ICCPR requires that states refrain from arbitrary and unlawful interferences with the privacy rights of individuals. The HR Committee has held that interceptions of private communications by Governments must be provided for by law, be in accordance with the provisions, aims and objectives of the Covenant and be reasonable in the particular circumstances of the case.[43] Criminalising data encryption facilitates the violation of privacy rights that in turn undermine the right to freedom of expression. The provision therefore violates both Article 17 and Article 19 of the ICCPR.

As no legitimate interest is engaged under the ICCPR, the measure cannot be said to be necessary or proportionate in the conduct that it penalises or the penalties that it provides.

Article 11 of the Cyber Crime Law provides aggravated sentences for Articles 8 to 10 where the crimes are directed against computer and communication systems used in public services with the intention of posing a threat to public peace and security.

Article 11 illuminates that neither Articles 8, 9 or 10 are tailored to protect a legitimate government interest. Instead, Article 11 provides for additional penal sanctions where such interests are threatened by acts prohibited under those three preceding Articles.

Article 11 cannot be said to meet the requirement of "prescribed by law" as its application is contingent on convictions under either Article 8, 9 or 10. Each provision fails to define the essential elements of the offense and do not require the showing of harm or damage. Individuals are therefore unable to determine what is and is not lawful under the provisions.

Article 11 purports to protect public peace and security, a legitimate aim protected by Article 19(3)(b) of the ICCPR. However, it is not narrowly tailored to be the least intrusive means of achieving this end. Johannesburg principle 15(1) states that individuals must not be punished for conduct unless actual or likely harm to national security flows from the prohibited act. Although Article 11 requires proving that an individual intended to threaten national security or public order, it does not require a showing of actual or likely harm. The imposition of criminal penalties in these circumstances is neither necessary nor proportionate.

Chapter Four – Crimes against Public Morality and Chastity

Article 14 of the Cyber Crime Law criminalises producing, sending, publishing, distributing, saving or financially engaging in obscene content by using computer or telecommunication systems or portable data storage devices.

As the title of chapter four suggests, this provision broadly restricts expression according to its content. The availability of the death penalty for this offense indicates the determination of the Iranian Government to suppress expression that it considers undesirable and makes Article 14 the most problematic provision in the Computer Crimes Law. As Article 19 of ICCPR is engaged, the restriction must be assessed against the three-part test: it must be prescribed by law; pursue a legitimate aim;

[43] *Antonius Cornelis Van Hulst v. Netherlands*, Communication No 903/1999 (at paragraph 7.3).

and be proportionate and necessary. The provisions of Article 14 failed to meet this test for the following reasons.

First, Article 14 is not prescribed by law because it is not formulated with sufficient precision to enable an individual to regulate his or her conduct according to the law. The elements of producing, sending, publishing, distributing, saving and financial engagement are not defined or distinguished from one another. The mental state required for criminal culpability in relation to any of these acts is not specified. Two separate attempts are made to define the malleable concept of obscenity. Note 1 proposes that materials containing pornographic or immoral scenes or images are obscene, essentially replacing one undefined term with two more. Note 4 elaborates that obscene materials include real or unreal images, audio recordings or writings that show full nudity of a woman or a man, their genitals or their engagement in a sexual act. Terms such as "immoral" and "pornographic" are impermissibly vague and what is meant by "full nudity" and "engagement in a sexual act" is left to the fertile imagination. Affording law enforcement agencies this degree of discretion while not providing the public with an accessible and certain vision of the prohibition violates Article 19 of the ICCPR.

Second, Article 19(3) of the ICCPR requires that restrictions on freedom of expression pursue a legitimate aim. The Iranian Government may argue that Article 14 protects the Article 19(3)(b) interest in public morals. General Comment No.34 states that the determination of what constitutes 'public morals' must not be based on principles deriving exclusively from a single tradition.[44] Rather it should be understood in the light of the universality of human rights and the principle of non-discrimination. Article 14 may violate Article 19 if it is applied to impose the values held by the government or theocratic elite rather than reflective of the diversity of views held within society. Further, the pluralism that is essential in a democratic society requires that people, even when in the majority, tolerate speech that they deem offensive. The ICCPR envisages a high threshold for when offensive speech reaches a degree of harm that would warrant a restriction on expression. Article 14 imposes blanket prohibitions on a spectrum of expression without clearly articulating a discernable threshold standard that distinguishes offensive expression from that which causes actual harm to society. Article 14 appears to provide a legal framework for the imposition of a singular conception of morality rather than a mechanism for protecting the public from harm. As such it cannot be said to pursue a legitimate aim.

Third, Article 19(3) of the ICCPR requires that restrictions on freedom of expression be necessary and proportionate. Restrictions must respond to a pressing need in a democratic society and by the least restrictive means available. The restriction must also be proportionate, in that the benefit to the protected interest outweighs the harm to freedom of expression. It is unclear what "pressing need" the Article 14 restriction meets in a democratic society. General Comment No.34 provides that legitimate restrictions on freedom of expression must demonstrate in a specific and individualised fashion the nature of the threat and establish a direct and immediate connection between the expression and the threat. Article 14 is not narrowly tailored to prevent specifically articulated harms and offers no mechanism for determining them. Rather, the definitions given to key terms such as obscenity appear to be deliberate and even cynical in their ambiguity. The consequence is essentially a blanket prohibition on the production, distribution and possession of any visual, audio or textual reference however oblique to nudity and human intimacy. This feasibly encompasses a virtually limitless spectrum of legitimate and harmless expression. The breadth of harm caused to freedom of expression far outweighs any tangible benefit to society. Article 14 cannot be said to be necessary or proportionate in these respects and it therefore falls short of the Article 19(3) of the ICCPR standard.

The proportionality requirement also applies to sentencing. Article 14 provides that those convicted be sentenced to 91 days up to 2 years in prison and/or a fine of 5 million Rials to 40 million Rials. Minimum sentences are the equivalent of mandatory sentences and do not provide the judge with the discretion to tailor the sentence to the nature of the offense and harm caused. Bizarrely, Note 1 contains assurances that those committing the acts listed in Article 14 will "definitely" receive the allocated punishments. This brings into question the legal effect of the mandatory sentencing

[44] Paragraph 32, HR Committee General Comment 34.

provisions in other Articles that appear categorical but lack such assurances. Note 2 provides for mitigation where fewer than 10 individuals receive distributed content. In these circumstances only reduced fines are available and custodial sentences are not. This apparent liberalisation is outweighed by Note 3, which provides that individuals engaged in Article 14 acts "professionally or systematically" will face both maximum punishments of 40 million Rials and 2 years in prison. An exception exists for individuals found to be "*mofsed-e fel-arz*" ("corrupt on earth"). This carries the death penalty and ambiguously applies to those who endeavour to promote and expand corruption on earth. This can be understood as any conduct that causes the degeneration, destruction and deviation of the society from its natural course. The concept has been used thus far in Iran as a catchall indictment of political dissent. The criminalisation of political dissent directly contravenes Article 19 ICCPR as it is never permissible to suppress expression on this basis. It follows that it is never proportionate to impose the death penalty to punish the exercise of expression, irrespective of the degree of harm caused. Article 6 ICCPR states that the death penalty can only be imposed for the most serious of crimes, which must be interpreted narrowly with the view to effect the global abolition of the death penalty.[45] ARTICLE 19 emphatically opposes the death penalty, particularly for crimes related to freedom of expression.

Article 15 of the Cyber Crime Law criminalises the use of computers, telecommunication systems or portable data storage devices for inciting or aiding and abetting in the commission of crimes.

Subparagraph (a) relates directly to Article 14, applying to those who provoke, encourage, threaten, invite, deceive, train or facilitate other individuals' access to obscene content. This is essentially accessorial liability for the principal offense contained in Article 14. The criticisms of Article 14 can therefore be applied here with one degree of separation. The issues of defining and determining obscene expression remain and it is not clear how these provisions protect public morals in conformity with Article 19(3)(b) ICCPR. This provision, like Article 14, is not prescribed by law, does not pursue a legitimate aim and therefore cannot be necessary or proportionate.

Subparagraph (b) criminalises the use of computers, telecommunications or portable data storage devices to provoke, encourage, threaten, invite, deceive or train individuals to "engage in such acts as rape, drug abuse, suicide, sexual perversion or violence."

The lack of definitions for the forms of assistance given or the acts assisted with lend this provision considerable ambiguity. Assistance in the form of expression may be legitimately restricted under Article19(3) of the ICCPR to protect the rights of others and public order. In particular it would be legitimate to criminalise expression that actually incites or creates an imminent danger of a person raping another or engaging in other violent acts. Expression assisting drug abuse, suicide, and sexual perversion feasibly includes a range of consensual and non-exploitative conduct the prohibition of which serves no legitimate protective end. Criminalising invites of "sexual perversion" may inhibit a whole range of harmless and consensual conduct. This ambiguity may also allow for the harassment of individuals that provide harm-reducing services to vulnerable people. For example, a drugs counsellor may be convicted of "encouraging drug abuse" or a public health worker advising on safer-sex could be convicted of "training individuals in sexual perversion". In respect of these latter restrictions it cannot be said that a legitimate aim is pursued and Article 19 of the ICCPR is therefore violated.

A footnote to Chapter Four qualifies both Article 14 and Article 15 with the assurance that neither provision applies to content "produced, developed, presented, distributed or published for scientific or other reasonable purposes." ARTICLE 19 finds these provisions inadequate in terms of the requirement of recognizing the public interest in freedom of expression and narrowly tailoring all restrictions in recognition of that interest. Its terms are too vague to assure the Iranian public that they can engage in legitimate expression without risk of prosecution. It provides no guidance on the meaning of "reasonable purposes" or the relevant factors in reconciling legitimate expression with criminal provisions that are antithetical to the right to freedom of expression. It is unlikely that this note would

[45] HR Committee, General Comment No. 6.

provide a sound legal footing for mounting a public interest defence. The note is therefore inadequate for redressing the profound deficiencies with Chapter Four as a whole.

This footnote illuminates the way in which the Computer Crimes Law entrenches restrictions on freedom of expression as norms while treating the right to freedom of expression as the exception. This subversion of values demonstrates the conceptual failure at the heart of the Computer Crimes Law.

Chapter Five – Disrepute (dishonour) and Dissemination of Lies

Article 16 of the Cyber Crime Law criminalises the use of a computer or telecommunication system to alter or manipulate someone else's image, audio or video file and publish it in a way that brings disrepute to that person as perceived by common law.

Article 16 criminalises a specific form of defamation where a person's right to a reputation is infringed through the alteration or manipulation of data relating to them. ARTICLE 19 has consistently advocated for the global abolition of criminal defamation laws. The HR Committee has similarly urged all states party to the ICCPR to consider abolishing their criminal defamation laws.[46] This advocacy position is strongly supported by a legal analysis of criminal defamation laws against the three-part test of Article 19(3) of the ICCPR. Such provisions, including Article 16, can rarely be said to be prescribed by law, pursue a legitimate aim and be necessary and proportionate.

Article 16 is formulated with insufficient clarity to be considered prescribed by law. The failure to define terms such as "altering" or "manipulating" and the omission of the requisite mental state for these acts makes it difficult for individuals to modify their conduct in conformity with the law. If Iran is to retain this criminal defamation law, it must at a minimum provide that the person manipulating or altering the data in question did so with knowledge of or a reckless disregard for the false impression the expression creates. In addition, it must be shown that the defaming party specifically intended to bring the defamed party into disrepute. Criminal defamation prosecutions are inherently vulnerable to exploitation if left to government authorities to enforce. The law should safeguard against this danger by prohibiting public authorities from initiating prosecutions for criminal defamation claims.

As repeatedly mentioned, Article 19(3) ICCPR allows for the right to freedom of expression to be limited in pursuit of an exhaustive list of legitimate interests. The "rights of others" is one enumerated interest and includes the right to a reputation. It is therefore legitimate for the Iranian government to seek protection of this right through restrictions on free expression, subject of course to the third prong of the Article 19(3) test.

The third part of the test requires that restrictions on expression be necessary and proportionate. ARTICLE 19 maintains that all criminal defamation laws are unnecessary and disproportionate, in particular where custodial sentences are imposed. Necessity and proportionality require that a provision be narrowly tailored to use the least intrusive means available to achieve the legitimate aim. Essentially, the interest in protecting the individual's reputation must outweigh the interest that the public has in the right to free expression. Article 16 fails to provide this balance. The acts prohibited include a variety of conduct that is of immense value in a democratic society. For example, the manipulation and alteration of data may include the popular satirical device of image manipulation that conveys critical messages on issues frequently in the public interest. Audiences are capable of discerning the satirical message behind the manipulation or alteration and knowing that in most cases it conveys an opinion rather than an assertion of fact. Article 16 is too broad to acknowledge the public interest in such expression.

[46] Concluding observations on Italy (CCPR/C/ITA/CO/5); concluding observations on the Former Yugoslav Republic of Macedonia (CCPR/C/MKD/CO/2).

Narrow tailoring also requires that defamation laws provide defences to safeguard legitimate expression. Firstly, Article 19 of the ICCPR requires the incorporation of a defence of truth, confirmed by the HR Committee in General Comment No.34. It is important that a defamation law recognises that there is no human right to a reputation not merited by one's conduct. If a manipulation or alteration of data conveys a truth that reflects an individual's actual conduct, that individual has no legitimate interest in suppressing that expression irrespective of the harm caused. Secondly, Article 19 of the ICCPR requires that defamation laws provide for a public interest defence where the value of the expression to the public is greater than the harm caused to the individual's reputation. This defence is broader than the defence of truth as it potentially covers statements that are untrue but ought to be protected to safeguard a culture in which free and open debate is encouraged. The defence must attach particular weight to the public interest in expression that concerns public officials, who are expected to display a higher degree of tolerance.[47] In the absence of these defences Article 16 fails to strike an appropriate balance between the right to reputation and the right to freedom of expression and therefore violates Article 19 of the ICCPR.

Again, ARTICLE 19 reiterates that sentencing must also be proportionate. Article 16 requires mandatory minimum custodial sentences or fines. Note 1 to Article 16 provides for aggravated sentences where an alteration or manipulation is "obscene". The inadequacy of this term is discussed in relation to Article 14. Obscene defamation carries the grossly disproportionate penalty of 2 years in prison in addition to a fine of 40 million Rials.

Article 17 of the Cyber Crime Law criminalises the use of a computer or telecommunication system to publish or make available someone else's personal or family images, audio or video files, or secrets without their consent in a way that brings disrepute to that person.

Article 17 purports to protect both the right to a reputation and the right to privacy, which this comment deals with in turn.

As noted above, Article 19(3)(a) of the ICCPR allows for freedom of expression to be restricted to protect the rights of others, including reputation rights as protected by Article 17 of the ICCPR. However, the right to a reputation does not include the right to a reputation one does not merit, making it necessary for defamation laws to contain a defence of truth. However, if a defence of truth were incorporated to this provision it is likely that it would be successful in almost every instance. Images, and audio or video files that have not been altered or manipulated can only convey facts that have actually occurred and been recorded. The term "secrets" also implies undisclosed matters of fact. Unless the meaning or significance of these facts is misrepresented in their presentation, these disclosures would be truthful and therefore fall within the defence of truth. This provision lacks such a defence and therefore criminalises truthful expression that Article 19 ICCPR protects. However, if it were amended to comply with Article 19 ICCPR it would be superfluous.

Expression may also be limited under Article 19(3)(a) to protect an individual's right to privacy, which is also guaranteed by Article 17 of the ICCPR. A state is under a positive obligation to protect individuals from arbitrary and unlawful interferences with this right. It is clear that an individual would normally have a privacy interest in personal and family images, related data and material that they have chosen not to make public. The legal protection of this autonomy is essential in a democratic society. However, the privacy interests of the individual must be balanced against the right to freedom of expression, which is given particular weight where the expression is in the public interest. This balance must also acknowledge that public officials have a lesser expectation of privacy due to the greater public interest in their conduct. Article 17 is a disproportionate restriction on freedom of expression because it fails to provide a public interest defence for disclosures of private information.

[47] Paragraph 47, General Comment No. 34.

Article 18 of the Cyber Crime Law illogically conjoins two distinct crimes into one sentence. As the offenses raise different issues, this analysis separates the two crimes into Article 18A and Article 18B, although the actual structure of the legislation is rather more confusing.

Article 18A may be summarised as criminalising the use of a computer or telecommunications to "disseminate lies" with the intention of damaging the public, disturbing the public state of mind or disturbing the official authorities' state of mind.

Article 18A is both vague and overbroad: it is as all encompassing in its scope as the fluid concept of "lies". It is distinct from criminal defamation laws or blasphemy laws in that it does not limit itself to protecting reputations or a specific idea or tradition. It encompasses both of these things in addition to any expression that the executive determines incompatible with their understanding of the "truth". Criminalising the dissemination of lies directly prohibits the freedom of expression that the ICCPR as a whole is engineered to protect. Article 19 of the ICCPR is engaged and the restriction must therefore be assessed against the three-part test contained in Article 19(3) of the ICCPR.

Firstly, Article 18A is not prescribed by law because it is not formulated with sufficient precision to allow individuals to modify their conduct in accordance with its terms. No definitions are provided for any of the terms within Article 18. Individuals seeking to abide by the law can only speculate at what the government considers "truth" and what it considers to be "lies." Article 18 requires that lies be disseminated with the intent of achieving one of three ill-defined objectives: damaging the public; disturbing the public state of mind; or disturbing the official authorities' state of mind. This appears to be deliberately ambiguous as it grants law-enforcement authorities with unrestrained discretion allowing them to target any dissenting speech that they determine undesirable. The ICCPR would not consider this restriction on expression "prescribed by law".

Secondly, Article 18A does not pursue a legitimate aim. Narrow tailoring requires that restrictions be content specific and clearly pursue an Article 19(3) ICCPR objective. "Damaging the public" and "disturbing the public state of mind or that of the official authorities" are neither specific nor are they legitimate aims that can be protected by restrictions on expression. It may be argued that the measure is designed to combat threats to national security and public order. However, Principle 2 of the Johannesburg Principles states that restrictions sought to be justified on the ground of national security are illegitimate unless their genuine purpose and demonstrable effect is to protect the country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force. Prohibiting expression that intends to disturb the public authorities' state of mind appears to be a pretext for protecting the government from embarrassment or exposure of wrongdoing, to conceal information about the functioning of public institutions, or to entrench a particular ideology. The aim of Article 18A is therefore illegitimate under Article 19(3) ICCPR.

Thirdly, Article 18A is not necessary or proportionate. Article 19 ICCPR requires the party invoking the restriction to demonstrate a direct and immediate connection between the expression and the harm sought to be prevented. Article 18A requires only that a harm is intended, not that a harm is caused or is likely to result. As such, it prohibits expression that poses no threat to the interests purportedly protected. Article 18A also fails the proportionality requirement. It must be shown that the restriction is specific and individual to attaining a protective outcome and is no more intrusive than other instruments capable of achieving the same limited result. The ambiguity of "disseminating lies" and the obscurity of the harms sought to be protected against cannot be said to be specific or individual. Rather, those drafting the law appear to have intended its effect to be over-broad and as intrusive as possible. It is foreseeable that the "dissemination of lies" will be exploited to target human rights defenders, journalists and bloggers who frequently disseminate information that governments would rather suppress and dismiss as untruthful. The UNHRCm has held that it would be impermissible to prohibit information dissemination systems from publishing material on the basis that they cast a critical view of the government or the political social system espoused by the government.[48]

[48] *Supra note* 14.

Article 18B criminalises the use of a computer or telecommunication system to associate a natural or legal person, or official authorities with a lie, regardless of whether the victim befalls financial or mental damage.

Criminalising expression that associates an individual or entity with a lie is generally characterised as a criminal defamation law. As noted above (see comments to Article 16 of the Cyber Crime Law), ARTICLE 19, as well as a growing body of international standards, call for the decriminalisation of defamation.[49] Assessing this restriction under the three-part test of Article 19(3) of the ICCPR illustrates that Article 18B and criminal defamation laws like it pose numerous problems.

Firstly, Article 18B is not prescribed by law as it lacks the qualities of accessibility and clarity required by ICCPR Article 19(3) ICCPR. Its ambiguity confers unfettered discretion on law enforcement officials while affording individuals no reasonable opportunity to modify their conduct in accordance with its terms. It fails to specify a standard for finding he requisite criminal intent for defamation. To comply with international standards it must at least require that the person making a defamatory statement has knowledge or is reckless as to the falsity of the statement with the specific intent of causing harm towards the defamed party.

Secondly, Article 18B must pursue a legitimate aim. The protection of the rights of others, enumerated within Article 19(3)(a) of the ICCPR, includes the legitimate suppression of speech to protect an individual's right to a reputation. Article 18B is drafted far too broadly than the ICCPR permits. Neither public bodies[50] nor legal entities such as companies have reputations that attract human rights. As such, no defamation law, whether criminal or civil, can legitimately protect the reputations of such entities on a human rights basis under Article 19(3)(a) of the ICCPR. That is not to say that individuals within these entities do not enjoy the protection of the ICCPR. However, individuals who hold public office are expected to display a higher degree of tolerance towards false speech made against them provided its dissemination was not malicious.[51]

Thirdly, a restriction on freedom of expression must be necessary and proportionate. This requires narrow tailoring. ARTICLE 19 maintains the position that all criminal defamation laws are disproportionate. It is disproportionate in all circumstances to provide custodial sentences for criminal defamation laws. The shadow that criminal defamation laws cast on legitimate free expression, particularly in relation to public officials, far outweighs any benefits that such laws confer on individuals' rights to a reputation. The HR Committee's General Comment No.34 is less unequivocal on this issue, stating that criminal defamation must only be applied to the most serious of cases and that imprisonment is never an appropriate penalty for such speech. The HR Committee also comments that a criminal defamation law must provide defences of truth, as well as a public interest defence. Article 18B does not provide for either defense, and is therefore not narrowly tailored to achieve the legitimate aim of protecting reputations.

Custodial sentences of 91 days to 2 years in prison and/or a fine of 5 million Rials to 40 million Rials are available for both Article 18 offenses. Minimum sentences are the equivalent of mandatory sentences and do not afford the sentencing judge with the discretion to impose penalties proportionate to the offenses committed.

---

[49] Concluding observations on Italy (CCPR/C/ITA/CO/5); concluding observations on the Former Yugoslav Republic of Macedonia (CCPR/C/MKD/CO/2).

[50] General Comment 34, at Paragraph 38, referencing the Concluding observations on Costa Rica (CCPR/C/CRI/CO/5)

[51] General Comment No. 34, at Paragraph 47

Chapter Six – Penal (legal) Responsibility of Individuals

Article 20 of the Cyber Crime Law relates to the sentencing of legal persons for offenses in the Computer Crimes Law. Where a crime is attributed to a business or organisation, custodial sentences are substituted for judicial orders to close a business or organisation either temporarily or permanently. The duration or permanence of the closure depends on the maximum corresponding custodial sentence and whether the conviction is for a repeat offence.

ARTICLE 19 is concerned that judicial orders of this nature could be used as a political tool to target organisations that express views contrary to government policy. Media organisations, human rights groups and trade unions would be particularly vulnerable to judicial closure orders. It would never be legitimate or proportionate under Article 19(3) of the ICCPR to close an organisation either temporarily or permanently on the basis that their expression was disagreeable. Article 20 indicates that proportionality should be a part of this process, that sentences of legal persons should reflect the circumstances, outcomes and income generated from the offense. However, this assessment does not expressly require the sentencing judge to consider the public interest in the expression that constituted an offense, or the harm to the public interest in open and public debate that would be caused by a closure order. Legal entities would be entitled to the same public interest defences that an individual is entitled to.

Article 21 of the Cyber Crime Law imposes liability on Internet Service Providers (ISPs) that fail to filter Internet content that "generates crime". Intentional failure to filter criminal content as required by the Web Crime Committee leads to the liquidation of the ISP. Negligent failure to filter criminal content is punished by a gradation of fines depending on the number of prior offenses followed by judicial closure orders of varying lengths for the third offense and thereafter.

As private entities, ISPs lack the institutional expertise to make legal determinations regarding the legitimacy of restrictions on expression. The threat of criminal sanctions gives ISPs a commercial incentive to be over-inclusive in their filtering decisions and over-cautious in the expression they prohibit. No accountability mechanism balances this by promoting the public interest in free expression. Delegating law-enforcement powers to the private sector with such asymmetric incentives encourages a censorship culture to develop with its own self-perpetuating momentum. By establishing ISP liability in this manner, Article 21 tacitly extends the reach of the Computer Crimes Law further into the realm of legitimate expression.

The Iranian Government must ensure that ISPs are not charged with the responsibility of determining what is and what is not legitimate expression. Criminal liability must certainly not be imposed on these service providers for the content that passes through their systems. Rather, Article 19 of the ICCPR provides a positive obligation on states party to promote the right to freedom of expression by ensuring that ISPs refrain from filtering content. General Comment No. 34 states that any restrictions on systems that support communication, including ISPs, are only permissible to the extent that they are compatible with Article 19(3) ICCPR.[52] Where prohibitions are permissible, they must be content-specific. It is never proportionate to impose generic bans on the operation of ISPs.[53]

Article 22 of the Cyber Crime Law charges the judiciary with the responsibility of establishing a web crime committee at the General Prosecutor's Office. The committee will be chaired by the General Prosecutor and be composed of a number of representatives from Government ministries. The committee will meet every fortnight to consider complaints and make decisions with regard to filtered regulations. These decisions are final and cannot be appealed.

---

[52] General Comment No. 34, at Paragraph 43.

[53] *Ibid.*

As a public body, the web crime committee must conduct itself within the bounds of the ICCPR. Any restrictions on the freedom of expression sanctioned by the committee must adhere to the three-part test in Article 19(3) of the ICCPR. If the committee is guided in its decision-making by any of the provision in the Computer Crimes Law it is likely that the three-part test will not be met. Article 22 also ensures that there is no judicial accountability for decisions of the web crime committee. This violates Article 2(3) ICCPR and the requirement of judicial oversight and an effective remedy for parties whose rights have been denied.

Article 23 of the Cyber Crime Law requires ISPs to implement the orders of the web crime committee or face penal sanctions. It also imposes a reporting requirement on ISPs to inform the web crime committee when it encounters illegal content. Article 23 supplements Article 21, confirming the role of the ISP in Iran as an agent of the state and as an instrument of censorship. The illegitimacy of this function has already been analysed in relation to Article 21.

Article 24 of the Cyber Crime Law prohibits the use of an international scale bandwidth without a legal permit. Limiting bandwidth severely restricts the ability of individuals to access or disseminate information. Limits of bandwidth particularly restrict an individuals' ability to download or stream audio and video files. This provision is likely part of Government efforts to restrict access to alternative information sources, particularly news sites that are not State-controlled.

Requiring permits to access international scale bandwidth allows the Government to exercise control over who is able to access this information according to its own prerogatives. It is likely that permits are distributed according to the nature of an organisation's work and dependent on their support for the incumbent Iranian government.

The provision can be said to be prescribed by law as the conduct that it covers is as clear as it is unjustified. It imposes liability without fault for the use of international-scale bandwidth without a license. It would be helpful in terms of "accessibility" for this provision to reference the law or regulations that guide the allocation of permits and how one acquires one.

The provision cannot be said to pursue a legitimate aim under Article 19 (3) of the ICCPR. It does not protect the rights of others or safeguard national security, public order or public health or morals. It arbitrarily denies individuals access to information without regard to the nature of the information or the threat it poses to any of these legitimate interests. The custodial sentences and fines imposed by the provision would be disproportionate even if a legitimate aim were engaged. Article 24 is antithetical to the positive obligation that Article 19 of the ICCPR imposes on states party to safeguard the right to impart and receive ideas.

Chapter Seven – Other Crimes

Article 25 of the Cyber Crime Law contains three offenses related to the facilitation of other crimes contained within the Computer Crimes Law. The compatibility of Article 25 with the right to freedom of expression depends on which crime has allegedly been facilitated. As the majority of crimes within the Computer Crimes Law are not compatible with Article 19 of the ICCPR, it is likely that Article 25 will only be applied to aggravate already existing violations of the right to freedom of expression.

Chapter Eight – Aggravation of Punishments

Article 26 of the Cyber Crime Law provides for aggravated sentences where the crime is particularly wide-spread, systematic or involves government officials breaching their official responsibilities. The availability of a provision that aggravates sentences already grossly disproportionate and in violation of Article 19 of the ICCPR is particularly concerning.

Article 27 of the Cyber Crime Law provides that on an individual's third offense they may be blocked from Internet subscription, mobile telephone use, registration of public domain and electronic banking.

These electronic communication bans are calculated on the basis of repeat offending rather than repeat convictions. A person may therefore face an Article 27 ban if they are charged with multiple counts of an offense. Article 27 bans are imposed without reference to the severity of the offenses, but their length will be determined according to the prison sentence given.

ARTICLE 19 points out that banning access to electronic communications directly infringes on an individual's right to freedom of expression. It is particularly concerning that this punishment could feasibly used against those who persist in expression deemed unsuitable by the Iranian Government that is wholly legitimate under international law. Human rights defenders, journalists, bloggers, and artists would be particularly vulnerable to bans on access to communications.

Part Two: Civil Procedure

Chapter Two – Collection of Electronic Evidence

Chapter Two of the Cyber Crime Law contains provisions concerning the search and seizure of evidence that is suspected of being used in relation to Computer Crimes. ISPs are required to keep records of Internet traffic data and personal information of Internet users. Article 48 incorporates the regulations in place for surveillance of telephone conversations to the Internet. ARTICLE 19 does not have access to these regulations, hence, thorough analysis of this provision can be provided only upon further review of additional legislation.

Part Three: Other Regulations

Article 52 of the Cyber Crime Law charges the Ministry of Justice and Ministry of Information and Communications Technology with the task of developing international partnerships to fight computer crimes.

Given the fundamental flaws of the Cyber Crime Law, ARTICLE 19 urges any entity approached by the Iranian Government in furtherance of this objective to take note of the analysis contained in this Comment and deny any assistance that may help with the implementation of the Computer Crimes Law or the propagation of its values.

Article 53 of the Cyber Crime Law provides that where computer or telecommunication systems have been used to commit a crime not covered by the Computer Crimes Law, resort must be made to existing penal laws. Article 53 demonstrates that in the absence of the Computer Crimes Law there are many alternative means available for the Iranian authorities to target and suppress expression that it finds disagreeable. Amendments to the Computer Crimes Law must be complemented by significant reforms to the Iranian Constitution, the Press Law of 1986 and the Islamic Penal Code.

Conclusions and Recommendations

As indicated by the above discussion, the Cyber Crime Law is contrary to international human rights law and interpretive standards in multiple ways. At the same time, the problematic aspects of the Cyber Crime Law cannot be remedied by simple amendments. ARTICLE 19 believes that restoring the right to freedom of expression in Iran requires wholesale reform to redress the conceptual failure signified by the Computer Crimes Law as well as other legislation. Protection and promotion of freedom of expression must be reasserted as norms and limitations on free expression as the exception.

Therefore, ARTICLE 19 recommends the following:

- The Iranian Government must repeal the Computer Crimes Law in its entirety.
- Comprehensive legal reform must include amending the Iranian Constitution to safeguard freedom of expression and the repeal of provisions of the 1986 Press Law and Islamic Penal Code that restrict the legitimate exercise of this right.
- Iran must immediately abolish the death penalty and decline to impose custodial sentences for expression-related offenses, except of those permitted by international legal standards and with adequate safeguards against abuse.
- Iran must repeal any law that imposes liability on Internet Service Providers for the content of expression that passes through their systems.
- Iran must immediately release all who are imprisoned or detained for legitimate exercise of their right to freedom of expression.