ARTICLE 19

Iraq: Draft Informatics Crimes Law

October 2011

Legal analysis

Executive summary

In October 2011, ARTICLE 19 analysed the Draft Informatics Crimes Law of Iraq ("Draft Law") that assesses the Draft Law's compliance with Iraq's obligations under international human rights law. ARTICLE 19 finds the Draft Law fundamentally flawed from a freedom of expression perspective; and if adopted, it will significantly undermine the right to freedom of expression and freedom of information in the country. ARTICLE 19 recommends that the Iraqi Council of Representatives reject the Draft Law in its entirety.

The Draft Law is problematic at its inception; the purposes of the Draft Law cite multiple negative consequences of the "information revolution" without acknowledging the positive role technology performs in today's society, not least of all in enhancing the enjoyment of fundamental human rights. The Draft Law provides no guarantees for the right to freedom of expression or freedom of information.

ARTICLE 19 believes that the Draft Law fundamentally distorts the legitimate bases for imposing restrictions on the right to freedom of expression and access to information. Each provision pursues numerous disconnected and ill-defined objectives, several of which are either not legitimate grounds for restricting the right to freedom of expression or are overly broad.

For example, Article 3 of the Draft Law prohibits computer use that compromises the independence of the state or its unity, integrity, safety or any of its high economic, political, social, military or security interests. This essentially grants law enforcement an incomprehensibly broad power to censor any electronic expression it deems necessary. Article 3 is among a number of provisions that carry a maximum sentence of life imprisonment.

Article 6(4) of the Draft Law appears to prohibit the publication or broadcasting of any false or misleading facts with the intent to weaken trust in the electronic trading and monetary systems. This feasibly incorporates any expression that intends to encourage critical discussion of these systems and is a flagrant attempt to limit the right of people in Iraq to engage in political speech.

Moreover, the Iraqi Government purports to grant itself the legal authority to impose its own moral code on the people of Iraq. The broadest of these restrictions, Article 21(b), imposes severe custodial and financial penalties on "whoever violates principles, religious, moral, family, or social values … through information networks or computers." Again, this an impermissibly broad content-based restriction that targets a spectrum of innocuous and harmless expression that the state has no interest in regulating.

The Draft Law further erodes the rights to freedom of expression and freedom of information by criminalising electronic defamation (Article 22(3)) and by failing to protect the right of journalists to protect their sources (Article 13(1)(c)).

For these reasons, ARTICLE 19 requests that the Iraqi Council of Representatives reject the Draft Law in its entirety. In light of the criticism provided in this and previous analyses of other legislation related to freedom of expression, ARTICLE 19 calls on the Iraqi Government to engage in comprehensive legal reforms to safeguard fundamental human rights and adopt legislation that promotes and protects the rights rather than suppresses them.

Recommendations

1. The Iraqi Council of Representatives should reject the Draft Law in its entirety.
2. Civil society organisations and other stakeholders should withhold their support from the Draft Law.
3. The Iraqi Council of Representatives should engage in comprehensive reforms to Iraq's legal framework to guarantee the right to freedom of expression and freedom of information for everyone in Iraq.

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, please contact Barbora Bukovska, Senior Director for Law, barbora@article19.org, +44 20 7324 2500.

Introduction

In this analysis, ARTICLE 19 details its concerns regarding the Draft Informatics Crimes Law ("the Draft Law"), issued by the Presidential Council of Iraq in September 2011. The analysis outlines Iraq'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 ultimately reviews the Draft Law for compliance with Iraq's obligations under international law and makes a series of recommendations to bring Iraq into compliance with those standards.

ARTICLE 19 has extensive experience on working towards legal and policy reform in Iraq on matters concerning the protection of freedom of expression and freedom of information.[1] We have been involved in recent discussions on the development of legislation on the protection of journalists[2], the law on freedom of information[3] and the law on freedom of expression, freedom of assembly and the right to peaceful protest.[4] We are, therefore, well placed to understand the proposal of the Draft Law against the current political, social and legal context in Iraq.

This analysis finds that a significant number of provisions in the Draft Law fail to provide adequate legal protections to the right to freedom of expression and freedom of information, among other fundamental rights. Moreover, the Draft Law is organised in a manner that makes it difficult to navigate with single articles grouping together distinct behaviours in pursuit of unrelated purposes. This confusion is compounded by the lack of definitions provided for key terms in the law, making it difficult for the general public to understand the nature of prohibitions and affording law enforcement agencies significant discretion in pursuing their own imperatives.

Too often the Draft Law compromises the right to freedom of expression and freedom of information in favour of poorly defined interests articulated in over-broad terms that relate only loosely to the protection of legitimate state interests. The Draft Law pursues interests beyond cyber-security, but also seeks to protect public order; uphold the reputations of individuals; maintain the secrecy of public and private information; and police public morals. Few of these provisions comply with international human rights standards.

ARTICLE 19 urges all Iraqi parliamentarians, civil society and other stakeholders to reject the Draft Law in its entirety. Instead, all stakeholders should jointly advocate for adoption of comprehensive legal framework that would safeguard the right to freedom of expression and freedom of information in the country and creating an enabling to both media and civil society.

---

[1] In recent years ARTICLE 19 has produced numerous reports on the state of media freedom in Iraq. See, for example, Free Speech in Iraq: Recent Developments (London, August 2007), available at http://www.article19.org/pdfs/publications/iraq-free-speech.pdf. ARTICLE 19 has also conducted strategic litigation in the country; see amicus brief in the case of the President of the Intelligence Services v Alan Rusbridger and Gaith Salim Abd al Ahad (concerning a defamation case brought against a journalist and a newspaper by the Iraqi authorities), 18 January 2010 http://www.article19.org/pdfs/analysis/iraq-alan-rusbridger-and-gaith-salim-abd-al-ahad.pdf.

[2] ARTICLE 19 analysed two versions of the Draft Law on the Protection of Journalists; see, the draft version of the Draft Journalists Protection Law of Iraq from August 2009; available at http://www.article19.org/pdfs/analysis/iraq-comment-on-draft-journalists-protection- law.pdf; and the final version of the Law in September 2011, available at http://www.article19.org/resources.php/resource/2734/en/iraq:-law-on-journalists%E2%80%99-protection-fails-to-protect-rights. In 2010, ARTICLE 19 also developed a model Draft Law on the Protection and Regulation of Journalists and Media Workers as a means to comprehensively and coherently protect journalists in accordance with international human rights law.

[3] See ARTICLE 19, Comment on the Draft Law on Access to Information, January 2010; available at http://www.article19.org/pdfs/press/iraq-article-19-comments-on-draft-access-to-information-law.pdf.

[4] See ARTICLE 19, Comment on the Draft Law on Freedom of Expression, Assembly and Peaceful Protest, July 2011; available at http://www.article19.org/data/files/medialibrary/2266/11-07-14-LEGAL-iraq.pdf.

International Freedom of Expression Standards

The right to freedom of expression, including the right to freedom of information, is a fundamental human right. The full enjoyment of this right is central to achieving individual freedoms and to developing democracy, particularly in countries transitioning from autocracy to democracy. 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 Draft Law engages a number of international human rights provisions that form the basis of the legal analysis in the following section. 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")[5] 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.[6]

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.[7] Article 19 of the ICCPR guarantees the right to freedom of expression in its first two paragraphs:

> 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.

Iraq signed the ICCPR on 18 February 1969 and ratified it on 25 January 1971. As a state party to the ICCPR, Iraq 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.

The UN Human Rights Committee ("HR Committee"), as treaty monitoring body for the ICCPR, issued General Comment No.34 in relation to Article 19 on 21 June 2011.[8] General Comment No.34

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

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

[7] Article 2 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).

[8] See CCPR/C/GC/34; available at http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf.

constitutes an authoritative interpretation of the minimum standards guaranteed by Article 19 of the ICCPR. ARTICLE 19 welcomed General Comment No.34 as a progressive and detailed elucidation of international law related to freedom of expression and access to information.[9] It is contemporary to and instructive on a number of freedom of expression concerns raised by the Draft Law.

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.[10] 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 and take all necessary steps to foster the independence of these new media and to ensure access of individuals thereto.[11] This includes an obligation to ensure easy, prompt, effective and practical access to Governmental information that is in the public interest.[12] Default recourse to secrecy without individually assessing the public interest of that information therefore violates Article 19 of the ICCPR.

While the right to freedom of expression is fundamental, it is not guaranteed in absolute terms. Article 19(3) of the ICCPR permits limitations on the right that are necessary and proportionate to protect the rights or reputations of others, for the protection of national security or public order, or public health and morals. Restrictions on the right to freedom of expression must be strictly and narrowly tailored to achieve one of these objectives 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 prescribed by law, pursue a legitimate aim, and that they conform to the strict tests of necessity and proportionality.[13]

Restrictions on internet-based, electronic or other such information dissemination systems are only permissible to the extent that they are compatible with Article 19(3) of the ICCPR.[14] The three-part test therefore applies to internet-based and electronic restrictions as it would to restrictions on the traditional print media.

Article 19(3) of the ICCPR 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.[15] Ambiguous or overly broad restrictions on freedom of expression deficient in elucidating the exact scope of their application are therefore impermissible under Article 19(3).

Interferences with the right to freedom of expression must pursue a legitimate protective aim as exhaustively enumerated in Article 19(3)(a) and (b) of the 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

---

[9] See UN: ARTICLE 19 Welcomes General Comment on Freedom of Expression, 5 August 2011; available at http://www.article19.org/resources.php/resource/2631/en/un:-article-19-welcomes-general-comment-on-freedom-of-expression.

[10] *Supra note* 8, Paragraph 12, HR Committee General Comment No.34.

[11] *Supra note* 8, Paragraph 15, HR Committee General Comment No.34.

[12] *Supra note* 8, Paragraph 19, HR Committee General Comment No.34.

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

[14] *Supra note* 8, Paragraph 43, HR Committee General Comment No.34.

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

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

permissible restrictions be content-specific: it would be impermissible to close a website 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 principles developed by international experts in 1995, 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 also provides 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 by law.

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 Rapporteurs represent the United Nations, the Americas, Europe, and Africa.[20]

---

[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] *Supra note* 8, Paragraph 32, HR Committee General Comment 34.

[19] The UN 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 Mijatovic; and the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression, Faith Pansy Tlakula.

[20] Available at http://www.osce.org/fom/78309.

The Rapporteurs stress the transformative nature of the Internet in terms of giving a voice to billions of people around the world, significantly enhancing their ability to access information. They recognise the Internet's potential to promote the realisation of other human rights, such as public participation, as well as to facilitate access to goods and services. Further, they note that the imposition of criminal liability for expression-related offenses must take into account the overall public interest in protecting forums for free expression. On this rationale, the Rapporteurs state that no blanket content-based restriction for material disseminated on the Internet is permissible. Finally, the Rapporteurs also express concern that, even when done in good faith, efforts by governments to regulate for cyber security often fail to take into account the special characteristics of the Internet, with the result that they unduly restrict freedom of expression.

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 Iraq is not a signatory, the Convention provides a model for a cyber crimes law that complies with international human rights standards.

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

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

Analysis of the Informatics Crime Law

The Draft Informatics Crime Law ("the Draft Law") contains a number of provisions that engage the right to freedom of expression. The Draft law is divided into four chapters: definitions and goals; punitive provisions; procedures for collecting evidence, investigation and trial; general regulations and conclusion.

This analysis focuses on substantive provisions contained in the first two chapters that engage the right to freedom of expression, the right to access to information and related fundamental rights. Provisions that do not explicitly engage these rights are excluded from the analysis, but may be found in the text of the Draft Law in the Appendix to this analysis.

Goals of the Draft Law

Article 2 outlines three goals of the legislature in enacting the Draft Law: to provide legal protection for the legitimate use of computers and information networks; to punish the perpetrators of acts that violate the rights of users; and to prevent the abuse of this law in order to commit computer crimes.

The concluding paragraphs of the Draft Law, titled "purposes," lend more emphasis to the second and third aim while apparently abandoning the first. In these paragraphs, the legislators hold the "new information era" responsible for new risks to individuals and institutions, such as: targeted attacks on data and information; exposure of the private life of individuals; threats to national security and sovereignty; weakening the trust in new technology, and putting the creativity of the human mind in danger.

ARTICLE 19 is concerned that the concluding remarks of the legislators focus attention on the negative consequences that have flowed from the "new information era" while ignoring the positive impact technology has had on society. Indeed, the conclusion that human creativity is jeopardised by technology is unfounded, as creative individuals and industries have fostered new technologies to develop new media and dramatically broaden their audience base. No reference is made to the role of technology in enhancing freedom of expression through increased access to information, enhanced pluralism in public commentary and the promotion of greater public participation in politics.

We note that the Draft Law may incentivise restrictive enforcement of the law without due regard for human rights safeguards. The UN General Assembly[23] and the Council of Europe[24] have both recognised that cyber security should not be achieved at the expense of the enjoyment of fundamental human rights. As noted by the Special Rapporteurs, good faith efforts to regulate for cyber security too often result in undue restrictions on the right to freedom of expression.[25] The Draft Law appears to fit within this category.

ARTICLE 19 encourages the Iraqi Parliament to integrate protections for freedom of expression and freedom of information to the Iraqi legal framework, and provide positive examples of "legitimate" computer use in addition to the perceived threats of the new information era. Any legislation on this subject should encourage that where there is a conflict between the right to freedom of expression and

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

[24] *Supra note* 22, Convention on Cybercrime.

[25] 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

other interests the law pursues; that any restriction on the right is provided by law, pursue a legitimate aim, and be necessary and proportionate.

Recommendations

- The right to freedom of expression and the right to freedom of information should be expressly guaranteed in the Iraqi legal framework.
- The Draft Law should incorporate positive examples of technology's role in enhancing enjoyment of fundamental human rights.

Freedom of Expression and the Protection of National Security and Public Order

As outlined above, the protection of national security and public order is a legitimate ground for restricting freedom of expression where that restriction is prescribed by law, necessary in a democratic society and proportionate. The Draft Law contains a number of provisions that appear to justify restrictions on expression on the basis of protecting national security and maintaining public order, but fail to comply with the three-part test of Article 19 of the ICCPR.

Article 3(1) of the Draft Law criminalises the use of computers or information networks with deliberate intent to (a) compromise the independence of the state or its unity, integrity, safety or any of its high economic, political, social, military or security interests or (b) subscribe, participate, negotiate, promote, contract or deal with an enemy in any way in order to destabilise security and public order or expose the country to danger.

Article 4 of the Draft Law criminalises managing a website with the deliberate intent to (1) implement programs or ideas which are disruptive to public order or promote or facilitate their implementation (2) implement terrorist operations under fake names or to facilitate communications with members or leaders of terrorist groups (3) promote terrorist activities and ideologies or to publish information regarding the manufacturing, preparation and implementation of flammable or explosive devices, or any tools or materials used in the planning or execution of terrorist acts.

Article 6 of the Draft Law criminalises the use of computers and information networks with deliberate intent to (1) create chaos in order to weaken the trust of the electronic system of the state (2) provoke or promote armed disobedience, provoke religious or sectarian strife, disturb public order, or harm the reputation of the country … (4) broadcast or publish false or misleading facts with intent to weaken trust in the electronic financial, trading and monetary systems, or to damage the national economy or the financial trust of the state.

None of the articles listed above comply with the requirement of prescription by law. Each Article contains a number of distinct offences, the key elements of which are not apparent on the face of the law to either the general public or law enforcement. Each provision raises numerous threshold questions. For example, it is not clear what "dealing with an enemy" involves; how one implements a program disruptive to public order; how erroneous commentary on the economy must be before it weakens trust in it; or who "the country" is and how can it be said to have a reputation in human rights terms. The answer to each of these questions raises a multitude of other uncertainties. The only redeeming feature of these provisions is that they require proof of "deliberate intent", although when the *actus reus* of an offence is so unclear, this adds little clarity. ARTICLE 19 believes that to leave these determinations to law enforcement, or even to the judiciary, would lead to arbitrary results that would consequently chill free expression on these issues.

Similarly, the provisions fail to articulate a legitimate aim that fits within the exhaustive list provided by Article 19(3) of the ICCPR. They purport to protect a diverse range of generic community interests that are far broader than the narrow concepts of national security and public order as legitimate restrictions permitted by Article 19(3). The state is given the power to essentially control information across the

entire spectrum of "economic, political and social interests", including the authority to police vague values such as "trust in the electronic financial, trading and monetary systems." We recall that also General Comment No.34 states that it is not "generally appropriate to include in the remit of [laws protecting national security] such categories of information as those relating to the commercial sector, banking and scientific progress."[26] Elements in these Articles that are more directly linked to safeguarding public order or national security are ambiguous, particularly "implementing ideas disruptive to the public order" or "facilitating communications with members of leaders of terrorist groups."

To fit within the rubric of protecting national security or public order, and to meet the requirements of necessity and proportionality, the interests pursued by these provisions must be more narrowly tailored. The Johannesburg Principles provide authoritative guidance on narrow tailoring for provisions related to national security. Principle 2 states that the genuine purpose and demonstrable effect of a provision must be 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. In violation of these standards, Draft Law Article 3 does not resemble this high threshold, instead protecting illegitimate and vague concepts such as the state's "reputation", its generic "integrity", its "safety" and its "stability."

ARTICLE 19 points out that "public order" must be defined in a similarly narrow fashion. The Draft Law employs concepts of sectarian strife, disruption, and disturbance that feasibly fall beneath the threshold of public disorder that would legitimately necessitate restrictions on free expression. In an analogous case concerning limitations on the right to freedom of association to safeguard public order, the European Court of Human Rights held that the risk of causing tension between communities did not justify an interference with the exercise of the right.[27] Instructive guidance can also be found in the decisions of national courts. For example, in the United Kingdom's Public Order Act, at section 5, threatening, abusive or insulting speech is restricted. However, in order to restrict speech, it must be shown that the speech is more than merely offensive or annoying, and that it was intended or likely to cause violence or alarm or distress.[28]

International standards, reflected in the Johannesburg Principles, also require that there be a causal link between the prohibited expression and the national security threat that is averted by that prohibition. Principle 6 provides a model three-part test for this purpose, allowing expression to be punished as a threat to national security only if a government can demonstrate that: (a) the expression is intended to incite imminent violence; (b) it is likely to incite such violence; and (c) there is a direct and immediate connection between the expression and the likelihood or occurrence of such violence. Provisions that purport to safeguard public order must also demonstrate this causal connection between the prohibited expression and the prevention of public disorder.

Specifically in relation to restrictions on expression that aim to avert terrorist attacks, the four Special Rapporteurs on freedom of expression have provided guidance on the meaning of "incite" that is also centred on causality. Incitement should be understood as a "direct call to engage in terrorism which is directly responsible for increasing the likelihood of a terrorist act occurring, or to actual participation in terrorist acts … Vague notions such as providing communications support to terrorism or extremism, the "glorification" or "promotion" of terrorism or extremism, and the mere repetition of statements by terrorists, which does not itself constitute incitement, should not be criminalised."[29]

The Draft Law prohibitions concerning national security and public order do not require a showing of this causal link between the expression prohibited and the harm averted. Indeed, the provisions on

---

[26] *Supra note* 8, HR Committee General Comment 34, para 30.

[27] *Ouranio Toxo v Greece* (2007) 45 EHRR 277, ECtHR.

[28] *Percy v. DPP* [2002] Crim LR 835, DC.

[29] Joint Declaration on defamation of religions, and anti-terrorism and anti-extremism legislation http://www.osce.org/fom/35639

terrorism do exactly what the Special Rapporteurs advice against; they equivocally prohibit the promotion of ideology, the facilitation of communications for terrorists, and the publishing of information relating to various terrorist practices. By failing to tolerate subversive speech that falls beneath the threshold of incitement and neglecting to require a causal connection between the prohibition and the protective outcome, the provisions fail to meet international standards on freedom of expression.

Penalties must also conform to the requirements of necessity and proportionality. Articles 3, 4 and 6 of the Draft Law provide for custodial sentences up to life imprisonment in addition to or instead of a fine between 25 million Iraqi Dinars and 50 million Iraqi Dinars. Life imprisonment and fines of this magnitude for offenses that do not require a showing of actual harm or threat of harm are certainly excessive and would violate the proportionality requirement in all but the gravest of cases.

With this legislative arsenal, law enforcement authorities could claim the legal authority for censoring any critical commentary contrary to official government policy or innocuous expression that poses no actual threat to national security or public order as narrowly defined.

Recommendations:

- Articles 3, 4, and 6 of the Draft Law must either be scrapped or amended to require that only expression that is intended to and is likely to incite imminent violence is prohibited, and that the prohibition is likely to avert that violence.

Freedom of Expression and the Protection of Morals

A number of provisions in the Draft Law place content-specific restrictions on computer-based expression with the purported aim of protecting morals. As outlined above, the defence of public morals is a legitimate ground for restricting expression under Article 19(3)(b) of the ICCPR if that restriction prescribed by law, necessary and proportionate.

In violation of this requirement, Article 21(b) of the Draft Law is the broadest of the restrictions within this category, imposing severe custodial and financial penalties on "whoever violates principles, religious, moral, family, or social values … through information networks or computers." Article 22(2)(a) is similarly broad, prohibiting the establishment of "Internet websites that promote or encourage pornography or any programs, information, images or videos which breach public modesty and morals." In the same manner, Article 22(3) imposes liability on the electronic communication of "words, images, or voices to someone else involving cursing." These are all broad content-based restrictions on expression and are therefore subject to the three-part test of Article 19(3) of the ICCPR.

The Draft Law provides little guidance on the interpretation of these provisions. The offenses are difficult to distinguish, as the vague concepts of "religious, moral, family, or social values"; "public modesty and morals"; and "cursing"; are undefined. In addition, the mental states required for criminal culpability in relation to any of these acts are not specified; an individual may violate the law without intent or knowledge of their act violating these vague standards. Affording law enforcement agencies this degree of discretion while not providing the public with an accessible and certain vision of the prohibition violates the requirement of prescription by law.

As noted above, the protection of public morals is a legitimate aim under the ICCPR. However, these three provisions are premised on fluid concepts that the executive may exploit to censor dissent or impose its subjective values system without regard for the diversity of views held in society. ARTICLE 19 recalls that the HR Committee has stated that the concept of public morals should not be based on principles deriving exclusively from a single tradition, but be understood in the light of the universality

of human rights and the principle of non-discrimination.[30] In their 2008 Joint Declaration, the Special Rapporteurs said restrictions on freedom of expression should be limited in scope to the protection of overriding individual rights and social interests, and should never be used to protect abstract notions, concepts or beliefs, including religious ones.[31] The potential for the laws to be applied in this way renders their aim illegitimate.

The provisions of the Draft Law do not satisfy the requirements of proportionality and necessity in this respect. They bear no relation to the goals of the legislation as set out in Article 2, making the 'pressing need' of the restrictions indiscernible. Law enforcement are given the broadest terms of reference for oppressing expression, allowing them to target any contentious social, religious or political expression without regard to the harm this causes to individuals' rights. Indeed, the provision does not demonstrate a direct and immediate connection between the suppression of that particular expression and the avoidance of any specific individualised threat. For example, no attention is paid to the context of the expression, relevant factors such as the risk that vulnerable, sensitive or non-consenting audience will be exposed to the expression and harmed by it are not considered. The net effect is therefore likely to be counter-democratic: chilling free expression and restricting pluralism. The provisions therefore fail to meet the requirements of Article 19(3) of the ICCPR at each stage of the three-part assessment.

The penalties available include custodial sentences, in some cases a minimum of 12 months, and fines ranging between two and five million Iraqi Dinars. Even if a pressing need were engaged, none of these provisions or the penalties available are narrowly tailored to meet the requirements of proportionality.

Freedom of Expression and the Protection of Reputation

The ICCPR permits restrictions on freedom of expression to protect the rights of others, including the right to a reputation as protected by Article 17 of the ICCPR. Draft Law Article 22(3) criminalises the use of computers or information networks to relate words, images, or voices to someone else involving slander. The term slander appears to be used synonymously with libel to cover both forms of defamation.

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.[32] In their 2002 Joint Declaration, the Special Rapporteurs stated that criminal defamation laws were not justifiable and should be abolished and replaced, where necessary, with civil defamation laws.[33] General Comment No. 34 of the HR Committee affirms that all states parties to the ICCPR should consider the decriminalisation of defamation.[34] This advocacy position is strongly supported by a legal analysis of criminal defamation laws against the three-part test of Article 19(3) ICCPR.

Article 22(3) of the Draft Law is not prescribed by law as it does not define any of the key elements of the offense. Expression that "involves" slander is not obviously limited to the dissemination of false

---

[30] *Supra note* 8, Paragraph 32 HR Committee General Comment 34.

[31] Joint Declaration on Defamation of Religions, and Anti-Terrorism and Anti-Extremism Legislation 2008. Available at http://www.osce.org/fom/35639

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

[33] Joint Declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 10 December 2002; available at http://www.osce.org/documents/rfm/2004/10/14893_en.pdf.

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

information that brings an injured party into disrepute. The mental element of the offense is also not specified; i.e. whether knowledge or recklessness of the falsity of the slanderous statement is required, as it ought to be. This ambiguity grants too much discretion to law enforcement authorities, who may initiate prosecutions even without a complaint from the apparently injured party. It also creates uncertainty among the general public, particularly among political commentators, as to what expression is permissible and what is not.

The principles of necessity and proportionality require a defamation law to be narrowly tailored to safeguard legitimate expression. Article 22(3) of the Draft Law is too broad to satisfy this requirement as it provides no defences to protect legitimate expression. Firstly, Article 19 ICCPR requires the incorporation of a defence of truth, confirmed by the HR Committee in General Comment No.34, that recognises an individual has no legitimate legal interest in suppressing truthful allegations against them. It is important that a defamation law recognises that there is no human right to a reputation that is not merited by one's conduct. 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 false 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.[35]

In the case of criminal defamation laws, the law is inherently vulnerable to exploitation if left to the government authorities to enforce. If Article 22(3) of the Draft Law is to be retained, it should safeguard against this danger by only allowing private individuals to initiate prosecutions for criminal defamation claims.

Again, ARTICLE 19 notes that sentencing must also comply with the proportionality principle. Article 22(3) provides for imprisonment of up to two years in addition to fines of between three and five million Iraqi Dinars for the crime of making statements "involving slander". ARTICLE 19 maintains that all criminal sanctions for defamation are disproportionate; fines and prison sentences of the magnitude recommended by Draft Law Article 22(3) certainly violate Article 19 ICCPR.

Recommendations:

- Iraq should abolish all criminal defamation provisions; Article 22(3) of the Draft Law should not be adopted.

Confidential Data and the Protection of Whistleblowers

Two provisions within the Draft Law target the "misuse" of public and private information, seemingly to protect the confidential nature of that information. The broad terms of these provisions have the potential to inhibit the right of individuals to disclose information that ought to be in the public domain, or to overzealously protect privacy rights without providing appropriate safeguards for the right to freedom of expression.

Draft Law Article 13(1)(c) prohibits a person from leaking information that they know by reason of their position with the intent of harming someone, or to bring benefit to themselves, or to use that information for a purpose other than that which it was provided for. A penalty of between 5 million and 10 million Iraqi Dinars and 3 years imprisonment is provided.

Draft Law Article 19(1)(a), read in conjunction with 19(2), imposes a maximum sentence of seven years for public officials engaged in the same act where the information was gained illegally.

[35] Paragraph 47, General Comment No. 34

These provisions may be regarded as a form of official and industrial secrets protection applying to both public and private information. The term "by reason of their position" implies a situation in which an employee of a public or private organisation violates their terms of employment by releasing information gained in the course of their employment. This potentially violates international standards that require whistleblowers who promote accountability by disclosing information relating to misconduct be given legal protection from sanctions for engaging in that conduct.

The importance of protecting whistleblowers is recognised in international law. The United Nations Convention on Anti-Corruption[36] Article 33 provides that each state party shall consider incorporating into its domestic legal system appropriate measures to provide protection against any unjustified treatment for any person who reports in good faith and on reasonable grounds to the competent authorities any facts concerning offences established in accordance with this Convention. Iraq acceded to the convention on 17 March 2008. In their 2004 Joint Statement, the four Special Rapporteurs on freedom of expression called on governments to provide better protections for those who release "information on violations of the law, on wrongdoing by public bodies, on a serious threat to health, safety or the environment, or on a breach of human rights or humanitarian law should be protected against legal, administrative or employment-related sanctions if they act in good faith."[37]

The Draft Law Articles 13(1)(c) and 19(1)(a) in conjunction with 19(2) fail to provide any legal protections for whistleblowers. Iraq is therefore not in compliance with the United Nations Convention on Anti-Corruption and the Draft Law fails to meet international standards as outlined by the Special Rapporteurs' Joint Declaration on this topic.

Recommendations:

- Iraqi legislation should provide protection for individuals who blow the whistle on public or private wrongdoing in accordance with Iraq's obligations under the UN Convention on Anti-Corruption.

Access to Information

Draft Law Article 21(1)(b) prohibits anyone from accessing a private website of a company or institution with the intent to change the design on this website, modify it, change it, delete it or *use it unduly* for his or her benefit or for the benefit of someone else.

ARTICLE 19 believes that the criminalisation of utilising a website "unduly" may have detrimental impacts on the right to freedom of expression or freedom of information. "Undue" use of a website may include innocuous and objectionable use of information for unforeseen purposes or use of a website in the commission of a serious offense. On the face of the law it is impossible to discern what type of conduct this provision intends to prohibit or what interest it seeks to protect. It is therefore impermissibly vague.

Recommendations:

- The criminal offense of "undue" use of a website should be removed from Draft Law Article 21(1)(b).

Protection of Journalists' Sources

[36] Adopted in General Assembly Resolution 58/4 of 31 October 2003

[37] Joint Declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression. December 2004.

Two provisions in the Draft Law require that individuals disclose information to the authorities on request, raising significant questions regarding the right to privacy. There are serious consequences for the right to freedom of expression, in particular the lack of an exception for journalists who seek to maintain the anonymity of their sources.

Article 13(3) of the Draft Law provides financial penalties of between 3 million and 5 million Iraqi Dinars for whoever refuses to provide the judicial, security and other relevant authorities with requested documents, that essentially includes any form of "information". Article 18(1)(b) appears to replicate this provision but refers specifically to electronic information. The following comments on Article 13(3) therefore apply equally to Article 18(1)(b).

Article 13(3) appears to provide a limitless police power on an unspecified "authority" to request and take property from any person, irrespective of whether there are reasonable grounds to suspect their involvement with an offence. It is not clear that this body requires any judicial permission, e.g. in the form of a warrant, to enforce their requests for information, or whether the body is subject to any judicial oversight. Without accountability this body is likely to abuse its powers in a way that may have the knock-on effect of discouraging people from seeking and maintaining information records on subjects they perceive the state as having an interest in. This directly interferes with an individuals right to privacy under Article 17 of the ICCPR and is consequently likely to impact enjoyment of the right to freedom of expression and access to information under Article 19 of the ICCPR.

More specifically, Article 13(3) of the Draft Law contains no exceptions for journalists who are required to protect the anonymity of their sources. In many instances, anonymity is the precondition upon which information is conveyed to a journalist. Protecting a journalist's right to protect their sources is therefore central to maintaining a free press fully capable of exercising its watchdog function in society, to expose official corruption and corporate wrongdoing. Denying this right also undermines the individual journalist and sources right to freedom of expression and access to information, and potentially puts their personal security in jeopardy. The European Court of Human Rights has held that the obligation of a journalist to protect their source's identity can only be denied in certain narrow circumstances where mandated by an overriding public interest.[38]

From a comparative perspective, ARTICLE 19 also recalls that the Committee of Ministers for the Council of Europe has issued recommendations on when the journalists' privilege may be overridden.[39] The explanatory memorandum provides that this may only be done in "exceptional circumstances where vital public or individual interests are at stake and can be convincingly established."[40] The reasoning of the Council of Europe can similarly be applied to the ICCPR. The reasons for compelling a journalist to disclose their sources must correspond to and not exceed the legitimate grounds for restricting expression under Article 19(3) ICCPR. To compel a journalist to disclose their source the authority must demonstrate that alternative measures to gain that information do not exist or have been exhausted. Additionally, they must show that the public interest in disclosure clearly outweighs the public interest in non-disclosure. The Council of Europe anticipates that a journalist may be required to disclose their sources if necessary to protect human life, to prevent major crime or in the defence of a person accused of having committed a major crime.[41] In addition, only a judicial body should have the power to compel a journalist to disclose their sources.

---

[38] Goodwin v. the United Kingdom, 27 March 1996, Application No. 17488/90 (European Court of Human Rights).

[39] Recommendation No. R (2000) 7 of the Committee of Ministers to member states on the right of journalists not to disclose their sources of information, adopted 8 March 2000.

[40] Council of Europe Committee of Ministers, Explanatory Memorandum to Recommendation No. R (00) 7 of the Committee of Ministers to member states on the right of journalists not to disclose their sources of information, para 28.

[41] Council of Europe Committee of Ministers, Explanatory Memorandum to Recommendation No. R (00) 7 of the Committee of Ministers to member states on the right of journalists not to disclose their sources of information, para 37-41.

Hence, Article 13(3) of the Draft Law falls short of international standards on respect for the right to freedom of expression and the right to privacy. Specifically it poses particular problems for the protection of journalists' sources and is likely to undermine media freedom in Iraq.

Recommendation

- Article 13(3) should be scrapped, or significantly amended to conform with international standards on respect for privacy, freedom of expression and the protection of journalists' sources.

Appendix: Text of the Draft Informatics Crime Law

In Name of the People

The Presidential Council

Based on what the parliament has passed and what was endorsed by the Presidential Council and the provisions of item (I) of Article (61) and item (III) of Article (73) of the Iraqi Constitution,

The following law has been issued

No. ( ) for the year 2010
Informatics Crimes Law

Chapter 1) Definitions and Goals

Article 1)
The following words and terms shall be defined as such for the purposes of this law:

(A) Computer: any device or interconnected group of devices for the purpose of conducting automated data processing.

Second) Automated Data Processing: the processes and tasks that are subject to computer data including their generation, sending, reception, storage or processing in any other way.

Third) Computer Data: this includes facts, information, concepts or any other means used in any form to carry out automated processing of data such as programs and systems.

Fourth) Programs: a set of commands that makes the system capable of performing automated processing of data.

Fifth) Information Network Service Providers: Any person or legal entity which provides users with internet services that allow computers to communicate. It also includes any other person handling stored data on behalf of the service provider.

Sixth) Passkeys: Includes the sets of characters and numbers needed for accessing networks, devices and computers or any header sent from or to an Access Point including the date, size, time of connection and information identifying the location which data is being transferred from or to. This incorporates all means of communications including cellular telecommunications.

Seventh) Subscription Data: it is the information requested by the service provider to identify and determine the physical address or the account information of the subscriber or the user of the service. This includes any information about the network, devices, individuals, computers, metadata, services, fees or where the devices are physically located if different from the location provided by Login Credentials.

Eighth) Electronic Cards: includes any credit cards, debit cards or any other payment card issued by an entity authorized by law.

Ninth) Information Network: Any group of computers or information-processing systems interconnected with each other to share data and information such as private networks, public networks and the Internet.

Tenth) Electronic Signature: a personal mark in the form of letters, numbers, symbols, signs, sounds or other means having a unique style which indicates its relation to the site and is approved by a certification agency.

Eleventh) Electronic Media: Includes electric, magnetic, optical or electromagnetic media, or any similar media which enables the creation and processing of information, exchange and storage.

Twelfth) Information: includes data, text, images, shapes, sounds, icons, databases and computer programs and the like which are created, stored, processed or sent by electronic media.

Thirteenth) Electronic Mail: a letter containing information which is created, attached, saved, transmitted or received in whole or in part, by electronic, digital, optical or any other media.

Fourteenth) Information Processing System: an electronic system used to create, send, receive, process or store information messages in any manner.

Fifteenth) Digital Certificate: a certificate issued by a licensed agency to testify the matching of an electronic signature to a specific person based on documentation procedures supported by law.

Article 2)

This law aims to provide legal protection for the legitimate use of computers and information networks, to punish the perpetrators of acts which violate the rights of users whether they may be individuals or legal entities and to prevent the abuse of this law in order to commit computer crimes.

Chapter 2) Punitive Provisions

Article 3)

First) A penalty of life imprisonment and a fine of not less than (25,000,000) twenty five million Iraqi Dinars and not more than (50,000,000) fifty million Iraqi Dinars shall be sentenced on whoever uses computers or information networks with deliberate intent to commit one of the following acts:

(A) Compromise the independence of the state or its unity, integrity, safety, or any of its high economic, political, social, military or security interests.

(B) Subscribe, participate, negotiate, promote, contract or deal with an enemy in any way in order to destabilize security and public order or expose the country to danger.

(C) Damage, cause defects, or hinder devices, systems, software, or information networks belonging to security, military or intelligence authorities with a deliberate intention to harm the state's internal or external security, or expose it to danger.

Second) Anyone who deliberately uses computer hardware, software, systems or information networks which belong to security, military or intelligence agencies with the deliberate intention to harm them, copy from them to send to an enemy, take advantage of them to carry out crimes against the state's internal or external security, or conceal such crimes shall be liable to the penalty provided in clause (First) of this article.

Article 4)

A penalty of life imprisonment and a fine of not less than (25,000,000) twenty five million Iraqi Dinars and not more than (50,000,000) fifty million Iraqi Dinars shall be sentenced on whoever establishes or manages a website with deliberate intent to commit one of the following acts:

First) Implement programs or ideas which are disruptive to public order or promote or facilitate their implementation.

Second) Implement terrorist operations under fake names or to facilitate communication with members or leaders of terrorist groups.

Third) Promote terrorist activities and ideologies or to publish information regarding the manufacturing, preparation and implementation of flammable or explosive devices, or any tools or materials used in the planning or execution of terrorist acts.

Article 5)

A penalty of life imprisonment and a fine of not less than (30,000,000) thirty million Iraqi Dinars and not more than (40,000,000) forty million Iraqi Dinars shall be sentenced on whoever commits one of the following acts:

First) Creates or publishes a website on the Internet for the purpose of human trafficking, or facilitates or promotes it in any form, or helps make deals or negotiations with the intention to perform human trafficking in any form.

Second) Creates or publishes a website on the Internet for the purpose of trafficking, promoting, or facilitating the abuse of drugs or psychotropic substances and the likes, or contracts, deals or negotiates with the intention to carry out transactions relating to trafficking in any form.

Article 6)

A penalty of temporary or life imprisonment and a fine of not less than (25,000,000) twenty five million Iraqi Dinars and not more than (50,000,000) fifty million Iraqi Dinars shall be sentenced on whoever uses computers and information networks with deliberate intent to commit one of the following acts:

First) Create chaos in order to weaken the trust of the electronic system of the state.

Second) Provoke or promote armed disobedience or threaten to do so. Provoke religious or sectarian strife, disturb public order or harm the reputation of the country.

Third) Deliberately damage, disable, defect, hinder or harm computer equipment, systems or information networks which belong to the state departments with intent to tamper with its system and infrastructure.

Fourth) Broadcast or publish false or misleading facts with intent to weaken trust in the electronic financial system or electronic trading and monetary currencies and the likes, or to damage the national economy or the financial trust of the state.

Article 7)

A penalty of temporary imprisonment and a fine of not less than (10,000,000) ten million Iraqi Dinars and not more than (30,000,000) thirty million Iraqi Dinars shall be sentenced on whoever commits the following:

First) Deliberately uses computers or information networks belonging to individuals, companies, agencies, banks or financial institutions and successfully steals other people's money, possessions, financial rights or achieves financial benefits for his/her self or someone else or deprives others of their financial rights by any means.

Second) Uses a computer or information network to seize programs, information, data or codes (for him/her self or for the benefit of someone else) of any electronic contracts or transactions, electronic cards, payments, money transfers, bonds or signatures on cheques using fraudulent methods or by using a fake alias or incorrect description to deceive the victim.

Third) Tampers, manipulates, changes or makes up data, invoices or programs which are related to stocks, bonds and currency rates traded within Iraq or data, invoices or programs which are used by constituencies within Iraq in activities on behalf of other parties related to stocks, bonds or currencies outside of Iraq.

Article 8)

First) Temporary imprisonment and a fine of not less than (10,000,000) ten million Iraqi Dinars and not more than (15,000,000) fifteen million Iraqi Dinars shall be sentenced on whoever commits the following acts:

(A) Forges, imitates or makes up by himself or using someone else, an electronic signature, bond or other writing or authentication certificate or a license for using digital signatures the like, or uses any of the above deliberately in an illegal manner.

(B) Forgers, imitates or makes up by himself or using someone else an electronic card or a smart card or any means which are used for local and foreign money transfers inside Iraq, or uses them, promotes them or deals with them while aware of their fraudulent nature.

(C) C. Uses or attempts to use a forged electronic card knowingly, or uses a forged card for pre-payment reservation knowingly.

(D) D. Deliberately makes up for himself or for someone else fake electronic data, documents, records or files or makes any manipulation or modification in any electronic document and uses any of them before a public or private constituency.

(E) E, Creates or posses, for the purpose of sale, distribution or display, programs, devices, data or any other technological method which can be used in forging, counterfeiting or manipulating with the intention or committing a crime or fraud.

Second) The acts mentioned in the First item of this Article would have a penalty of imprisonment for not less than ten (10) years and a fine of not less than (20,000,000) twenty million Iraqi Dinars and not more than (30,000,000) thirty million Iraqi Dinars if the acts were:

(A) Concerning the rights of the state, public sector or private institutions which provide public benefit.

(B) Committed by an employee or someone in charge of public service while performing their job or because of it.

Article 9)

First) The penalty of imprisonment for not more than (10) ten years and a fine of not less than (5,000,000) five million Iraqi Dinars and not more than (10,000,000) ten million Iraqi Dinars shall be sentenced on whoever steals, possesses or deliberately seizes an electronic signature, a writing, documents, records or electronic financial trading and monetary currencies or any electronic invoices which are related to the rights, wealth or properties of others, for the sake of seeking benefit for him/her self.

Second) The penalty of temporary imprisonment and a fine of not less than (3,000,000) three million Iraqi Dinars and not more than (5,000,000) five million Iraqi Dinars shall be sentenced on whoever is entrusted with the devices, programs, data, information networks, electronic cards or any electronic invoices, whether he/she has been appointed by the public authorities to protect them as a secretary or a guard and he/she seizes them with the intention to possess or to utilize for his/her own benefit or the benefit of someone else or has achieved earnings from them in an illegal manner.

Article 10)

A penalty of imprisonment for not less than seven (7) years and a fine of not less than (10,000,000) ten million Iraqi Dinars and not more than (30,000,000) thirty million Iraqi Dinars shall be sentenced on whoever establishes, manages, promotes or publishes a website on the internet which allows or facilitates money laundering through illegal monetary operations such as fake bank transfers, virtual transactions or transfers, exchanges, uses, obtains or possesses money through illegal electronic means or by hiding the money's sources while knowing that it came from illegal sources.

Article 11)

First) A penalty of imprisonment for not than seven (7) years and a fine of not less than (3,000,000) of three million Iraqi Dinars and not more than (5,000,000) five million Iraqi Dinars shall be sentenced on whoever commits the following acts:

(A) Threatens someone using computers and information networks to commit a felony against him/her self or against his/her properties or against someone else's property in order to threaten someone into taking or abstaining from a certain action.

(B) Sends or transmits any message, news, or electronic documents through computers or information networks which contains information which implies a threat or blackmail for a person to take or abstain from a certain action.

Second) For all the cases of threats or blackmail using computers and information networks not mentioned in the First item in this article, the penalty would be temporary imprisonment and a fine of not less than (2,000,000) two million Iraqi Dinars and not more than (4,000,000) four million Iraqi Dinars.

Article 12)

First) A penalty of temporary imprisonment and a fine of not less than (3,000,000) three million Iraqi Dinars and not more than (5,000,000) five million Iraqi Dinars shall be sentenced on whoever establishes, publishes or presents a false digital signature certificate.

Second) A penalty of temporary imprisonment for not less than three (3) months and not more than (1) one year or a fine of not less than (30,000,000) thirty million Iraqi Dinars and not more than (50,000,000) fifty million Iraqi Dinars shall be sentenced on whoever practices issuing digital signature certificates illegally.

Article 13)

First) A penalty of imprisonment for not less than three (3) years and/or a fine of not less than (5,000,000) five million Iraqi Dinars and not more than (10,000,000) ten million Iraqi Dinars shall be sentenced on whoever:

(A) Deliberately damages or destroys an electronic signature, medium or mail.

(B) Deliberately uses an electronic writing, mail, medium or signature, contrary to their terms and conditions of use.

(C) Anyone who due to his/her position knows data of electronic signatures or electronic media or information and leaks them with the intent to harm someone or to bring benefit to him/her self or someone else, or uses them for a purpose different than the purpose for which they were provided.

(D) Gains unauthorized access in any way to an electronic signature, medium or mail or hacks media or intercepts or disables them from performing.

Second) A penalty of temporary imprisonment and a fine of not less than (3,000,000) three million Iraqi Dinars and not more than (10,000,000) ten million Iraqi Dinars shall be sentenced on whoever provides false information to a digital certificate issuing agency with the intent to obtain, suspend or cancel a certificate.

Third) A fine of not less than (3,000,000) three million Iraqi Dinars and not more than (5,000,000) five million Iraqi Dinars shall be sentenced on whoever refuses to provide the judicial, security and other relevant authorities to submit all requested documents including licenses, reports, information, statistics, data, records, electronic trading and monetary currencies, software or any other electronic invoices and as long as it is relevant to the activities carried on, and does not violate the rights of intellectual property.

Article 14)

First) A penalty of imprisonment not more than three (3) years or a fine of not less than (10,000,000) ten million Iraqi Dinars and not more than (15,000,000) fifteen million Iraqi Dinars shall be sentenced on whoever commits the following acts:

(A) Damages, defects or disables an electronic bond or an electronic card that is currently in credit or reservation, or has done so to any other financial or property rights or any other electronic mail used to prove these electronic rights.

(B) Uses electronic trading and monetary currencies, electronic records, electronic cards or any invoices related to computers and information networks in his/her business, which include rights of others, and neglects organizing these records.

Second) A penalty of imprisonment for not less than three (3) years and/or a fine of not less than (15,000,000) fifteen million Iraqi Dinars and not more than (25,000,000) twenty five million Iraqi Dinars shall be sentenced on whoever deliberately disables, damages or obstructs computer hardware, software or information networks which are made for the public benefit.

Third) A penalty of imprisonment for a term not more than three (3) months or a fine of not less than (2,000,000) two million Iraqi Dinars and not more than (5,000,000) five million Iraqi Dinars shall be sentenced on whoever:

(A) Has been assigned the task of operation and supervision of a computer and due to his/her mistake causes damage, defect, or obstruction to computer hardware, operating systems, software or information networks and the likes.

(B) Intrudes, annoys or calls computer and information network users without authorization or hinders their use. Deliberately accesses a website, an information system, a computer system or a part of one without authorization. Uses or facilitates the use of computers belonging to others, directly or indirectly without authorization.

(C) Benefits unduly from telecommunications services through information networks or computers.

Article 15)

First) A penalty of temporary imprisonment and a fine of not less than (10,000,000) ten million Iraqi Dinars and not more than (15,000,000) fifteen million Iraqi Dinars shall be sentenced on whoever commits one of the following acts:

(A) Deliberately trespasses an authorized-access-only area or intercepts any information while it is being transmitted.

(B) Spies or follows data and information whether stored in or being transmitted between information systems.

Second) A penalty of imprisonment for not less than (4) four years and a fine of not less than (15,000,000) fifteen million Iraqi Dinars and not more than (25,000,000) twenty five million Iraqi Dinars shall be sentenced if any act described in the First item of this Article leads to the destruction, deletion, modification, defecting, disabling, or republishing of data and information belonging to others unduly.

Article 16)

A penalty of imprisonment for not more than seven (7) years and/or a fine of not less than (25,000,000) twenty five million Iraqi Dinars and not more than (50,000,000) fifty million Iraqi Dinars shall be sentenced on whoever receives or intercepts unduly whatever is sent from a computer or information network, for the purpose of using it for financial benefits for him/her self or for someone else.

Article 17)

First) A penalty of imprisonment for a term not more than three (3) years and a fine of not less than (5,000,000) five million Iraqi Dinars and not more than (10,000,000) ten million Iraqi Dinars shall be sentenced on whoever removes or disables an encryption to an electronic signature, a computer, an information network, or an electronic card belong to someone else with the intent to commit any crime mentioned in this law.

Second) A penalty of temporary imprisonment and a fine of not less than (10,000,000) ten million Iraqi Dinars and not more than (15,000,000) fifteen million Iraqi Dinars shall be sentenced if any of the crimes mentioned in the First item of this Article are committed on computer hardware, software, records, electronic cards or rights of the state departments, public institutions or those working on its behalf.

Article 18)

First) A penalty of temporary imprisonment or a fine of not less than (5,000,000) five million Iraqi Dinars and not more than (10,000,000) ten million Iraqi Dinars shall be sentenced on whoever commits one of the following acts:

(A) Knowingly provides false electronic information or data to judicial or security authorities.

(B) Refuses to provide electronic information or data to the judicial or security authorities.

Second) A penalty of imprisonment not more than three (3) years and a fine of not less than (2,000,000) two million Iraqi Dinars and not more than (3,000,000) three million Iraqi Dinars shall be sentenced on whoever commits one of the following:

(A) Uses computers and information networks to and pose under title or alias which he/she is not entitled to with the intent of deception or fraud.

(B) Creates or uses a fake website or hides the truth behind a website on the internet or assists in doing such with intent to commit one of the crimes mentioned in this law.

Third) A penalty of imprisonment for a term not more than seven (7) years and a fine of not less than (15,000,000) fifteen million Iraqi Dinars and not more than (20,000,000) twenty million Iraqi Dinars shall be sentenced if crimes mentioned in the First and Second items of this Article are committed by a public employee or someone in charge of a public service or if the fake title, or information are related to a public employee or governmental department.

Article 19)

First) A penalty of imprisonment for not less than three (3) years and a fine of not less than (5,000,000) five million Iraqi Dinars and not more than (10,000,000) ten million Iraqi Dinars shall be sentenced on whoever commits one of the following acts:

(A) Illegally obtains information, data, programs or computer output and leaks them or deliberately publishes them using computers and information networks with the intent to harm someone.
(B) Reveals any type of information related to subscribers, secrets or login credentials to any third party without legal approvals issued from the relevant official department.
(C) Sells, copies or exchanges personal information provided by individuals to him/her for any reason without their permission with the intent to obtain financial benefits for him/her self or for others.

Second) A penalty of imprisonment for not more than seven (7) years and a fine of not less than (5,000,000) five million Iraqi Dinars and not more than (10,000,000) ten million Iraqi Dinars shall be sentenced if any of the crimes mentioned in the First item of this Article are committed by a government employee or someone in charge of a public service during performance of his/her duties or because of them.

Article 20)

First) A penalty of imprisonment and a fine of not less than (2,000,000) two million Iraqi Dinars and not more than (5,000,000) five million Iraqi Dinars shall be sentenced on whoever uses computers and information networks to commit one of the following acts:
(A) Uses, with the intention to defraud, a trademark registered in Iraq for someone else as the title of his website on the Internet or facilitates such action to a company working in the field of IT in Iraq.
(B) Uses an electronic card to make a reservation while knowing that it has insufficient funds. Or Uses it after its expiry or cancellation knowingly, or uses an electronic card which belongs to someone else without the knowledge of his owner.

Second) The penalty for the crimes mentioned in the First item this article would become imprisonment for not more than ten (10) years and a fine of not less than (5,000,000) five million Iraqi Dinars and not more than (10,000,000) ten million Iraqi Dinars in one of the following two cases:
(A) If the offender was a government employee or in charge of a public service and has committed any of the offenses set forth in the First item of this article while performing his/her duty or because of it, or has facilitated it to others.
(B) If the acts mentioned in the First item of this Article were used against any computer system or information network which belongs to any governmental agency in the Republic of Iraq, or against computers belonging to any agency which represents them.

Article 21)

First) A penalty of imprisonment for not less than (2) years and not more than three (3) years and/or a fine of not less than (10,000,000) ten million Iraqi Dinars and not more than (20,000,000) twenty million Iraqi Dinars shall be sentenced on whoever commits one of the following acts:
(A) Publishes or copies through computers or information networks any scientific research work, literary or intellectual properties which belong to someone else and is protected by international laws and agreements.
(B) Accesses a private website of a company or institution to with the intent to change the design on this website, modify it, change it, delete it or use it unduly for his/her benefit or for the benefit of someone else.

Second) A penalty of a fine of not less than (500,000) five hundred thousand Iraqi Dinars and not more than (1,000,000) million Iraqi Dinars shall be sentenced on whoever copies, publishes or shares unlicensed software or information.

Third) A penalty of imprisonment for not less than a year and a fine of not less than (2,000,000) two million Iraqi Dinars and not more than (5,000,000) five million Iraqi Dinars shall be sentenced on whoever violates principles, religious, moral, family, or social values or personal privacy through information networks or computers in any way.

Article 22)

First) A penalty of imprisonment for a term not more than three (3) years and a fine of not less than (3,000,000) of three million Iraqi Dinars and not more than (6,000,000) six million Iraqi Dinars shall be sentenced on whoever establishes, manages or assists the establishment of a website on the internet for gambling or gambles or promotes gambling using the information networks.

Second) A penalty of temporary imprisonment and a fine of not less than (10,000,000) ten million Iraqi Dinars and not more than (30,000,000) thirty million Iraqi Dinars shall be sentenced on whoever commits one of the following acts:

(A) Establishes, manages or assists the establishment of a website on the internet to promote or encourage pornography or any programs, information, images or videos which breach public modesty and morals.

(B) Exposes a juvenile or a child to activities which breach morals or modesty or uses the internet to promote, produce or distribute pornography or prepares or organizes activities or phone calls which breach modesty which involve a juvenile or a child using emails, information networks or computers.

Third) A penalty of imprisonment for not more than (2) years and/or a fine of not less than (3,000,000) three million Iraqi Dinars and not more than (5,000,000) five million Iraqi Dinars shall be sentenced on whoever uses computers or information networks to relate words, images, or voices to someone else involving cursing or slander.

Article 23)

A penalty of imprisonment for not less than (1) year and not more than (2) years and a fine of not less than (3,000,000) of three million Iraqi Dinars and not more than (5,000,000) five million Iraqi Dinars shall be sentenced on whoever deliberately produces, sells, imports or distributes any devices, tools, computer software, hardware, passwords or login information which leads to committing one of the crimes mentioned in this law.

Chapter 3) Procedures for Collecting Evidence, Investigation and Trial

Article 24)

First) Investigation authorities shall take responsibility for carrying out investigation procedures and evidence collections and requesting them from their sources regarding all crimes mentioned in this law.

Second) Investigation authorities may not begin search procedures without a warrant from the judge responsible for their case.

Third) The judge of the investigation or the investigator shall take responsibility in carrying out the procedures of seizing and collection evidence as well as any other investigative procedure stipulated in the law of Code of Criminal Procedure.

Article 25)

First)

(A) The Criminal or Misdemeanour Court of Ar-Rusafa district shall be the specialized court responsible for looking into cases of all the crimes mentioned in this law for a period of three (3) years from the date of issuing of this law according to its specialization.

(B) The court mentioned in paragraph A shall continue to look into the cases raised to it until they are thoroughly done and have reached a final sentence.

*Second)*After the period mentioned in the First item of this Article has passed criminal courts and courts of misdemeanours shall take responsibility in accepting all cases of crimes mentioned in this law, according to their geographic relevance.

Third) One or more experienced and specialized judges who have received special training in the field of informatics crimes shall be responsible for judging crimes mentioned in this law.

Fourth) Any specialized judge in the phase of investigation or trial may seek technical assistance from inside or outside Iraq.

Article 26)

First) A specialized judge may:

(A) Issue orders for any third party to save computer data, including all information or data which is stored in the computer or its peripherals, add-ons or outputs whenever there is a probability that such information could be changed or lost.

(B) Issue orders to information network service providers or other technical service providers to provide subscription data or login credentials to the investigation authority if that would help reveal the crime.

(C) Access computers, information networks or any parts of them as well as stored data in them or in any medium in which data can be stored inside Iraq. They may also intercept data or monitor it with a purposeful order and for a specific time and purpose only.

(D) Track information all the way to computers or all other networks connected to the suspect computer given that all third parties who own these computers and networks are informed of the investigation's procedures and its range as long as the range of this procedure is limited to what is related to the investigation without violating or interfering with the rights and privacies of others.

(E) Seize computers, parts of them, or the media in which data was stored and transfer them to investigation authorities in order to have them analyzed and studied. They may also copy them without transferring the system and remove the data encryption which would prevent the data from being accessed, without harming the system, the program stored in it or the data.

Second) The authority responsible for collecting evidence may:

(A) Prepare two copies of data under analysis and study, one to be given directly to the responsible judge before carrying out the analysis and all analysis procedures shall be carried out on the second copy and no modification may be made to either of these copies.

(B) Submit electronic or hard copies or the evidence attached with a detailed report explaining the procedures which were followed, the tools and the devices which were used to obtain the information or retrieve it.

Third) Investigative authorities and expert authorities may submit outputs of electronic copies in digital format, attached with a detailed report with the date of the hard-copy retrieval procedure.

Chapter 4) General Regulations and Conclusion

Article 27)

Anyone found guilty of one of the crimes mentioned in this law shall be punished according to this law without discarding any greater punishment enforced by one of the other applicable laws.

Article 28)

First) Responsibilities of legal entities which are stipulated in the Penal Code number (111) of 1969 regarding crimes stipulated in this law which have been committed by legal entities or for their benefit shall be applicable.

Second) In the case that a crime was committed by an individual under the name of or for the benefit of a legal entity, the entity shall be committed to co-operate with the convicted individual in meeting the expectations of paying all dues, fines and compensations.

Article 29)

The court has the right to confiscate or destroy tools, devices or programs used in committing crimes mentioned in this law and it shall not be considered as a violation for the rights of other well-intentioned parties.

Article 30)

The following laws shall apply to any crimes not mentioned in this law:

First) The Penal Code number (111) for the year 1969

Second) The Code of Criminal Procedure number (23) for the year 1971

Article 31)
This Law shall be enforced starting from 90 days after its publication in the Official Gazette.

Purpose:
Whereas providing legal protection and the establishment of a punitive system for the perpetrators of computer and information networks crimes which accompanied the emergence, growth and development of computer systems, networks and information technology revolution has become necessary, and

Whereas this new information era has brought about many new risks to individuals and institutions, such as targeted attacks on data and information, exposure of the private life of individuals, threats to national security and sovereignty, weakening the trust in new technology and putting the creativity of the human mind in danger, and

In order to provide legal protection for computer systems on which the government is encouraging the public to rely and depend,

This law has been drafted.