DISCLAIMER
This document is a rough translation written in Arabic, which can be found at:
http://www.alhaq.org/arabic/index.php?option=com_content&view=article&id=868:-2017-&catid=86:2012-05-09-07-29-49&Itemid=201

20 September 2017

Al-Haq's Comments on the Law by Decree on Cybercrime of 2017

On 24 June 2017, President Mahmoud Abbas approved the Law by Decree on Cybercrimes (hereinafter Cybercrimes Decree Law), which had been referred to him by the government on 20 June 2017. The Cybercrimes Decree Law was published in the Palestinian Official Gazette (Issue 14) on 9 July 2017. Article 61 provides that the Cybercrimes Decree Law shall enter into force as of the date of its publication in the Official Gazette.

The publication, along with the mechanism used to discuss, approve and publish the Cybercrimes Decree Law, was received with opposition from Palestinian civil society organisations. The whole process was carried out in complete secrecy. Despite demands from civil society organisations to be involved in the discussion, concerned stakeholders including, *inter alia*, civil society organisations, national institutions, the Palestinian Journalists' Syndicate, Palestinian Bar Association, and internet service providers, did not review the Law or participate in relevant discussions. With the continued absence of the Palestinian Legislative Council (PLC), the authorised legislative body according to the Constitution, these demands still went unanswered. This approach is entirely inconsistent with the government-declared policy articulated in the National Policy Agenda 2017-22: Putting Citizens First. According to this document, the government stresses its commitment to full partnership with, and openness to, civil society.

The Cybercrimes Decree Law was not included in the minutes of the last session held by the Council of Ministers on 20 June 2017 despite the fact that the Preamble to the Decree Law references that session. The draft of the Cybercrimes Decree Law, which was published in the Official Gazette, was largely different and more severe from the drafts circulated earlier. The Cybercrimes Decree Law also provided that it shall enter into effect as of the date of its publication in the Official Gazette, contravening legal norms surrounding penal legislation which allow citizens ample time, as of the date of publication, to consider and comment on the Law before it enters into force. This is also in accordance with principles of transparency.

As such, the Cybercrimes Decree Law does not comply with the applicable approach to dealing with penal legislation. Instead, the published draft of the Cybercrimes Decree Law provides imprecise information. It further raises questions as to whether it is limited to this type of crime; in accordance with international standards; and if it is meant to

DISCLAIMER
This document is a rough translation written in Arabic, which can be found at:
http://www.alhaq.org/arabic/index.php?option=com_content&view=article&id=868:-2017-&catid=86:2012-05-09-07-29-49&Itemid=201

provide a pretext to violate public rights and freedoms, particularly the right to freedom of expression, right to privacy and right of access to information.

General comments on the Cybercrime Decree Law

1. Article 43 of the Amended Basic Law, necessity is a constitutional condition for any legislation, including the Cybercrimes Decree Law, to be valid. Before it was approved and published in the Official Gazette on 9 July 2017, the first draft of the Decree Law had been referred, together with an explanatory note by the Attorney General, to the Prime Minister on 17 October 2016. This lengthy process confirms that the requirement of "necessity that cannot be delayed" under the Basic Law was no longer viable. Given the lack of the required constitutional conditions, the Cybercrimes Decree Law cannot be characterised as an exceptional legislation.

2. According to the explanatory note attached to the Cybercrimes Decree Law, and which was referred to the Prime Minister on 17 October 2016, the Attorney General is the party that submitted the draft law. According to Article 43 of the Basic Law, the President of the Palestinian National Authority is the only stakeholder that is allowed to submit draft legislations to the government for discussion. The fact that the Public Prosecution submitted the draft entails a conflict of interests, evidenced by the broad powers the Cybercrimes Decree Law confers on the Public Prosecution in procedures. The Public Prosecution is an adversary in the crimes provided for by the Cybercrime Decree Law.

3. To a great extent, the Cybercrimes Decree Law goes beyond the limits of cybercrime, and encompasses many common crimes within the scope of cybercrimes. The Cybercrimes Decree Law further declares any crime as a cybercrime if committed through cyberspace which violates the International Convention on Cybercrime (Budapest Convention). Contrary to common legal norms, the Cybercrimes Decree Law adopts the method by which a crime is committed in order to aggravate the penalties of what it considers cybercrimes. By contrast, the Budapest Convention adopts the "nature of the offence" as in those offences related to confidentiality and integrity of electronic systems. The Convention is also concerned with "how widespread" cybercrimes are, including offences related to computers, content, and violations of copyright and related rights – as provided for in the Budapest Convention.

Effective since 2004, the Budapest Convention is an international reference for relevant domestic legislation. The Convention lists four categories of cybercrimes: (1) offences against the confidentiality, integrity and availability of computer data and systems. This covers: illegal access by means of piracy, unauthorised password protection systems, taking advantage of software gaps, illegal data interception, violations of privacy by

DISCLAIMER
This document is a rough translation written in Arabic, which can be found at:
http://www.alhaq.org/arabic/index.php?option=com_content&view=article&id=868:-2017-&catid=86:2012-05-09-07-29-49&Itemid=201

transmitting computer data, data interference through malicious codes and viruses, the obstruction of lawful usage of computer systems, and the misuse of the devices used as a tool in cybercrime; (2) computer-related forgery, fraud and theft; (3) content-related offences, including offences related to child pornography; and (4) offences related to infringements on copyright and intellectual rights. A total of 13 thematic articles provide for penalties for the aforementioned cybercrimes under the Budapest Convention.

In addition, the 2010 Arab Convention on Combating Information Technology Offences (Arab Convention) not only provides for offences related to pornography involving children and minors, but also lists offences related to pornography in general. Furthermore, the Arab Convention prohibits offences related to terrorism committed by means of information technology, money laundering, drug trafficking, human and human organ trafficking, and illicit arms trafficking. Article 21 of the Arab Convention expands the scope of criminalisation to include all traditional offences when they are committed by means of information technology. This implies an unjustified extension of the scope of these types of offences. The Arab Convention is incompatible with the Budapest Convention's approach dealing with cybercrime. In fact, the Arab Convention seems to rather depend on the "method" to deal with cybercrimes. It is important to note that the Arab Convention has a total of 21 thematic articles that prescribe penalties for information technology offences. Meanwhile, the Palestinian Cybercrime Decree Law provides for a greater number of offences; a total of 45 thematic penal provisions. It is therefore imperative to adopt an approach based on the Budapest and Arab Conventions to deal with cybercrimes and which is in line with international standards.

4. The Cybercrime Decree Law uses several overly broad and loosely defined terms in several provisions. These are inconsistent with the fundamental principles of knowledge of legal norms and legality, as well as absolute clarity and balance between criminalisation and punishment, allowing for an unrestrained interpretation. The role of law enforcement agencies must be limited to investigating whether a criminal act has been committed or not. Such terms found in the Cybercrimes Decree Law include: "infringement on public morals", "endangering the integrity of the Palestinian state, the public order or the internal or external security of the State", "attacking family principles or values", "inciting racial hatred", "harming national unity", "harming social peace", etc. According to the Budapest Convention, these offences are beyond the concept of cybercrime.

Moreover, such offences cannot be included as part of the restrictions allowed for under Article 19 of the International Covenant on Civil and Political Rights (ICCPR) regarding the right to freedom of expression. The offences set in the Cybercrimes Decree Law cannot pass the strict three-part test of these restrictions to establish their legality in

DISCLAIMER
This document is a rough translation written in Arabic, which can be found at:
http://www.alhaq.org/arabic/index.php?option=com_content&view=article&id=868:-2017-&catid=86:2012-05-09-07-29-49&Itemid=201

accordance with international standards. Instead, the offences jeopardise the right to freedom of expression. The three-part test provides that any limitation must be provided for clearly and unambiguously in law. It further establishes that the restriction should aim to protect an overriding legitimate public interest and be governed by the standards of necessity and proportionality (European Court for Human Rights). A restriction should not pose a threat to the right to freedom of expression. Moreover, these restrictions must be familiar in a democratic society. In other words, when addressing such restrictions, courts must pay special attention to a set of principles and standards, which are grounded in respect for pluralism, tolerance, equality, freedom and promotion of self-realisation. Accordingly, those provisions of the Cybercrimes Decree Law, which do not stand the three-part test, must be ruled out because they infringe upon the right to freedom of expression.

This needs to be emphasised by adding a precautionary provision to the Cybercrimes Decree Law prescribing that: "It shall be prohibited to construe or interpret any provision under this Law by Decree in a manner that contradicts or infringes on the right to freedom of expression and the right to privacy enshrined in the international conventions the State of Palestine has acceded to, and other relevant international standards." It must also be stressed that the provisions of the Cybercrimes Decree Law should be practically interpreted according to the three-part test in order to safeguard public rights and freedoms, particularly the right to freedom of expression and the right to privacy.

5. Loosely-interpreted terms under many provisions of the Cybercrimes Decree Law can generate an increasing sense of restraint among journalists, bloggers, activists, and generally among citizens. Such terms can be detrimental to freedom of the press and the right of access to information. Such overly broad language negatively reflects on the public and generates fear. Overly broad terms can also result in an unjust enforcement of these provisions, solely at the discretion of law enforcement agencies. Ultimately, these terms may impinge on the rule of law, equality and non-discrimination.

6. Many penal provisions under the Cybercrimes Decree Law prescribe penalties on the basis of "intent" (*mens rea*) – the mental element of a criminal offence. In principle, intent cannot practically be established without the realisation of material element (*actus rea*), including the perpetration of the criminal offence, criminal consequence and causal link. As such, the elements of the crime are incomplete. For example, Article 20 of the Cybercrimes Decree Law establishes the creation or management of websites that *aim to* publish news that would endanger the integrity of the state, its public order or the internal or external security of the State as an offence. Also, Article 18 of the Law criminalises the creation of "websites, applications or electronic accounts or dissemination of

information on the electronic network with *the intent to* commit the offence of money laundering or to finance terrorism" (emphasis added).

7. Many penal provisions under the Cybercrimes Decree Law prescribe excessively severe penalties. Contrary to the principle of legality, these penalties are not informed by a presupposed balance between criminalisation and punishment. Under the Law, penalties can be as severe as hard labour, either temporarily or for life. For example, Article 51 of the Decree Law provides that "if any of the offences provided for under this Law by Decree is committed for the purpose of disrupting public order, endangering the safety and security of the society, or endangering the lives of citizens, or with the intention of harming national unity or social peace, the penalty shall be hard labour for life or temporary hard labour." The Law also imposes exorbitant fines, amounting to JD 5,000 or JD 10,000. In some instances, the Decree Law combines criminal penalties with fines within the same provision, contradicting general principles for the classification of penalties. Additionally, loosely defined terms are used in the context of severe penalties, violating the principle of legality and knowledge of legal norms. These penalties are also incompatible with the philosophy of punishment, which is grounded in correction rather than retaliation.

8. In relation to the proceedings of penal cases involving cybercrimes, a distinction should be made between online media outlets and other websites. This is in line with the provisions of Article 27 of the Basic Law, which explicitly prohibits "any restrictions" to be imposed on media outlets, unless the restrictions are in accordance with the provisions of the law and "judicial ruling". On the other hand, the Law also infringes on the norms and guarantees enshrined in the Penal Procedure Law in relation to communications surveillance. It also violates international standards, articulated by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, particularly those provided in the 2013 report submitted to the Human Rights Council (A/HRC/23/40).

9. The Cybercrimes Decree Law allows websites to be blocked in violation of relevant international standards, particularly the 2016 Human Rights Council Resolution (A/HRC/32/L.20). The resolution "[c]ondemns unequivocally measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law and calls on all States to refrain from and cease such measures". In this context, and without scant regard for the principle of proportionality, Article 40(2) of the Cybercrime Decree Law allows the Attorney General or one of his assistants to request a Magistrate Judge to block websites within 24 hours. Further, the Judge will be able to issue a judgement on the same day in relation to any offence provided for in the Cybercrime Decree Law, completely disregarding the principle of

proportionality. In other provisions such as Article 54, it seems that the court does not have a discretionary power to block websites. Instead, it only has the power to set the timeframe during which a website can be blocked. The court can only decide how long a website, in the instance of a cybercrime committed, will be blocked.

In addition, according to international standards, blocking websites requires a final court decision. A website may not be blocked during the course of investigation. The court decision should apply to more serious crimes, such as organised crime or child pornography, rather than to all offences provided for under the Cybercrimes Decree Law. Along this line, in 2011, a joint declaration on the freedom of expression and the Internet was issued by the UN and other international experts.[1]

Clause 3, "Filtering and Blocking," of the joint declaration states that "[m]andatory blocking of entire websites, IP addresses, ports, network protocols or types of uses (such as social networking) is an extreme measure – analogous to banning a newspaper or broadcaster – which can only be justified in accordance with international standards, for example where necessary to protect children against sexual abuse." Clause 6, "Access to the Internet," also provides that "[d]enying individuals the right to access the Internet as a punishment is an extreme measure, which could be justified only where less restrictive measures are not available and where ordered by a court, taking into account the impact of this measure on the enjoyment of human rights."

10. The Cybercrimes Decree Law also neglects the standards set by the International Principles on the Application of Human Rights to Communications Surveillance.

11. Although the Budapest Convention includes detailed provisions on the protection of copyright and related rights and criminalises violation of this right, which has been of global concern, the Cybercrimes Decree Law completely disregards this area.

Detailed comments on the Cybercrime Decree Law

1. Article 3(1) of the Cybercrime Decree Law provides that "a specialized unit for cybercrime shall be established in the police and security forces, provided that it has judicial authority. The Public Prosecution shall supervise the judicial control officers within their jurisdiction." Nothing justifies an unwarranted expansion of the mandate of security agencies, who already enjoy the mandate of judicial police, so as to include the

[1] This included: United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organisation for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organisation of American States (OAS) Special Rapporteur on Freedom of Expression, and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information

DISCLAIMER
This document is a rough translation written in Arabic, which can be found at:
http://www.alhaq.org/arabic/index.php?option=com_content&view=article&id=868:-2017-&catid=86:2012-05-09-07-29-49&Itemid=201

power to prosecute cybercrimes. Several Palestinian security agencies possess this capacity, including the General Intelligence, Preventive Security, Military Intelligence, Civil Defence, etc. This provision can result in overlapping powers and jurisdictions in the prosecution of cybercrime. It may also negatively impact the rights and guarantees under international and Palestinian law. It is therefore believed that this power should be given to the Palestinian police, who have a cybercrimes unit. According to the Palestinian Penal Procedure Law, the police agency is originally vested with judicial duties.

2. Article 6 of the Cybercrime Decree Law provides that "anyone who has produced, or deployed through an electronic network or an information technology means, anything that can stop it, disrupt it, destroy programs, delete, or modify them, will be sentenced to temporary hard labor and a fine of no less than five thousand JD, and no more than ten thousand Jordanian Dinars or the equivalent in the legally circulated currency." Firstly, this provision simultaneously prescribes a penalty for a criminal offence (temporary hard labour) and a fine. Secondly, the provision imposes an excessively harsh penalty, namely temporary hard labour. Contrary to the requirements set by the principle of legality, this penalty is disproportionate to the gravity of relevant offences. The provision does not make a distinction between legal devices and programmes that are produced or used to maintain security and protection of networks and information, and those which illegally cause damage, disruption or destruction of these devices and programmes by means of malicious codes, viruses, etc.

3. According to Article 8(2) of the Cybercrimes Decree Law, "any person who unlawfully uses personal encryption elements or the electronic signature creation tool to forge the signature of another person, shall be punished by imprisonment or by a fine of no less than two thousand Jordanian Dinars and no more than five thousand Jordanian Dinars or by a combination of both punishments." It is not clear what *unlawfully* means. Does it mean that a person needs to obtain permission, allowing the official authority to conduct secret surveillance on personal encryption and anonymity tools? The Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/HRC/29/32) highlights that "States should neither prohibit nor conduct secret surveillance on strong encryption and anonymity. National laws should recognise that individuals are free to protect the privacy of their digital communications by using encryption technology and tools that allow anonymity online. States should not restrict encryption and anonymity, which facilitate and often enable the rights to freedom of opinion and expression." Hence, the use of encryption elements or tools, whether personal or within the framework of one's work, is safeguarded by international human rights standards. Article 8(2) of the Law also prescribes an excessively severe penalty, namely temporary hard labour, against any person who *unlawfully* uses personal encryption elements. Once again, the provision combines penalties for both criminal offences and misdemeanours.

DISCLAIMER
This document is a rough translation written in Arabic, which can be found at:
http://www.alhaq.org/arabic/index.php?option=com_content&view=article&id=868:-2017-&catid=86:2012-05-09-07-29-49&Itemid=201

4. While the Cybercrimes Decree Law provides for excessively harsh penalties, the penalties themselves are also inconsistent with other legislation. For example, Article 13 prescribes temporary hard labour against a person "who uses an electronic network or any other type of information technology to steal or embezzle funds." This penalty is not necessarily proportionate to the nature of the committed offence. By contrast, under the Penal Law, theft can be a criminal offence if it involves aggravated circumstances. Otherwise, it is characterised as a misdemeanour. Contrary to the categories of penalties provided by the general rules of penal legislation, Article 13 of the Cybercrime Decree Law prescribes a misdemeanour penalty (a fine) together with a criminal penalty.

5. Pursuant to Article 15(1) of the Cybercrime Decree Law, "anyone who uses the Internet or an information technology device to threaten or blackmail another person to carry out an act or to refrain from doing so, even if such an act or omission is lawful, shall be punished by imprisonment or by a fine of no less than two thousand Jordanian Dinars and no more than five thousand Jordanian Dinars or by a combination of both punishments." The terms *threaten* and *blackmail* are vague. According to Article 15, "*to threat or blackmail*" is effected to compel another person to perform an act or omission. Even if such an act or omission is lawful, it will be criminalised. In such a case, even advocacy campaigns to amend the Cybercrimes Decree Law could fall within the purview of the Law.

Article 15(2) also incorporates overly broad and loosely defined terms, such as a threat to commit "a felony or to attribute dishonourable acts" and prescribes an excessively harsh penalty, namely temporary hard labour if the threat concerns perpetration of a crime or an act of morally offensive content. The same provision involves penalties for both crimes and misdemeanours. The terms used in this provision need to be defined.

6. Article 16 of the Cybercrimes Decree Law provides: "1. Anyone who has produced any material that infringes upon public morals, or has arranged, prepared, sent or stored it for the purpose of exploiting, distributing or presenting it to others through the electronic network, an information technology means, or animated cartoons shall be punished by imprisonment for a period no less than one year, a fine of no less than one thousand Jordanian Dinars and no more than five thousand Jordanian Dinars, or by both penalties. 2. Any person who creates a website, an application or an electronic account, or who publishes information on the Internet or on another information technology platform in order to facilitate programs and ideas that infringe upon public morality shall be punished by imprisonment for a period of at least one year or by a fine of no less than one thousand Jordanian Dinars and no more than five thousand Jordanian Dinars or by a combination of both punishments." In several respects, these provisions clearly violate personal freedom and the right to freedom of expression. The term *public morals* is overly broad

and violates the three-part test, which assesses controls on the right to freedom of expression.

In addition, the Article in question renders the right to freedom of expression meaningless. Criminalisation on the mere grounds of producing, preparing, arranging, transmitting, storing or presenting material to others, impinges on personal freedoms. According to the Human Rights Committee's General Comment 34 on Article 19 of the ICCPR, "the concept of morals derives from many social, philosophical and religious traditions; consequently, limitations... for the purpose of protecting morals must be based on principles not deriving exclusively from a single tradition. Any such limitations must be understood in the light of universality of human rights" Against this background, Article 15(1) of the Cybercrime Decree Law criminalises many acts that fall within the framework of the right to freedom of expression and personal freedoms. Under Article 15(2), the phrase "facilitating programmes and ideas that promote and infringe on public morals" may also establish as criminal offences many acts associated with the right to freedom of expression. In this context, the Budapest Convention narrowly restricts criminalisation to those acts which involve child pornography. To sum up, Article 15 of the Cybercrime Decree Law needs to be discarded from the scope of cybercrimes because it bears grave consequences on the right to freedom of expression and personal freedoms.

7. Article 20 of the Cybercrimes Decree Law provides: "1. anyone who creates or manages a website or an information technology platform that aims to publish news that would endanger the integrity of the Palestinian state, the public order or the internal or external security of the State shall be punished by imprisonment for a period of at least one year or by a fine of no less than one thousand Jordanian Dinars and no more than five thousand Jordanian Dinars or by a combination of both punishments. 2. Any person who propagates that news by the any means, including broadcasting or publishing it, shall be sentenced to a maximum of one year in prison, be required to pay a fine of no less than two hundred Jordanian Dinar and no more than one thousand Jordanian Dinars or be subjected to both penalties."

These provisions also violate the principle of legality and individuals' right to know legal norms, on the grounds of which their behaviour is assessed. These terms allow for multiple interpretations, potentially implying an infringement on the right to freedom of expression. In light of relevant international standards, Article 20 of Cybercrimes Decree Law cannot stand the three-part test for controls on the right to freedom of expression. On the basis of this article, the Public Prosecution detained five journalists. It was also invoked by the court to extend the detention of these journalists. The offence provided for by Article 20 does not fall within the scope of cybercrimes under the Budapest Convention. According to paragraph 43 of General Comment 34 of the Human Rights Committee, "[t]he penalisation of a media outlet, publishers or journalist solely for being

DISCLAIMER
This document is a rough translation written in Arabic, which can be found at:
http://www.alhaq.org/arabic/index.php?option=com_content&view=article&id=868:-2017-&catid=86:2012-05-09-07-29-49&Itemid=201

critical of the government or the political […] system espoused by the government can never be considered to be a necessary restriction of freedom of expression."

8. In accordance with Article 21 of the Cybercrimes Decree Law, "Anyone who creates a website, an application or an electronic account, or disseminates information on the Internet or an information technology device with the intention to offend or to violate a sacred or religious rite or belief shall be punished by imprisonment for a period of at least one year or by a fine of no less than two thousand Jordanian Dinars and no more than five thousand Jordanian Dinars or by a combination of both punishments." This article incorporates a loosely defined expression, namely "offending or violating a sacred or religious rite or belief." It involves an unjustified restriction of the right to freedom of expression, which might be in the form of criticism of religions and religious scholars. This offence is under the Budapest Convention. According to General Comment 34 of the Human Rights Committee, it would not be "permissible for […] prohibitions to be used to prevent or punish criticism of religious leaders or commentary on religious doctrine and tenets of faith."[2]

9. Pursuant to Article 22 of the Cybercrimes Decree Law, "Anyone who creates a website, an application, or an electronic account, or publishes information on the Internet or an information technology device with the intent to attack any family principles or values by publishing news, photos, audio or video recordings, whether directly or indirectly, relating to the inviolability of private and family life, even if it is true, in order to defame others and harm them, shall be punished by imprisonment for a period of at least two year or by a fine of no less than three thousand Jordanian Dinars and no more than five thousand Jordanian Dinars or by a combination of both punishments."

Article 22 uses overly broad expressions, e.g. "attack any family principles or values." Moreover, Article 22 does not make a distinction between libel and slander directed at public figures and ordinary people. With regards to those directed at public figures, regulations need to show a significant degree of lenience. If it is expressed with no bad faith, libel and slander, then it should not be criminalised and rather redressed by means of civil compensation. In its General Comment 34, the Human Rights Committee explicitly highlights that "States parties should consider the decriminalisation of defamation and, in any case, the application of the criminal law should only be countenanced in the most serious of cases and imprisonment is never an appropriate penalty;" Here defamation is considered libel and slander under Palestinian legislation. Furthermore, in many joint declarations, the UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur on Freedom of Expression and ACHPR Special Rapporteur on Freedom of

[2] Paragraph 48 of General Comment

DISCLAIMER
This document is a rough translation written in Arabic, which can be found at:
http://www.alhaq.org/arabic/index.php?option=com_content&view=article&id=868:-2017-&catid=86:2012-05-09-07-29-49&Itemid=201

Expression and Access to Information have repeatedly called on all States to abolish penal defamation laws. In particular, these three international officials stated in their 2002 joint declaration that "all criminal defamation laws should be abolished and replaced, where necessary, with appropriate civil defamation laws."

10. According to Article 24 of the Cybercrimes Decree Law, "Anyone who establishes a website, an application or an electronic account, or who publishes information through the computer network or any other information technology platform for the purpose of publishing and disseminating information that incites racial hatred, provokes racial discrimination against a particular group, or threatens aggression against someone because of their ethnic or sectarian affiliation, color, looks or cause of disability shall be sentanced to temporary hard labor and a fine of no less than five thousand Jordanian Dinars and no more than ten thousand Jordanian Dinars or the equivalent thereof in the legally circulated currency." This article uses loosely defined expressions, such as "incitement to racial hatred" which are inappropriate to serve as a penal provision. Article 24 also implies an unjustified restriction of the right to freedom of expression. In practice, monitoring and documentation provided by Al-Haq and other human rights organisations has demonstrated that such a provision is invoked to arrest journalists and citizens on grounds of expressing their opinion. In addition, the article prescribes excessively severe penalties, which are not proportionate to the nature of the offences committed.

11. Article 26 of the Cybercrime Decree Law provides that "Whoever acquires any device, program, electronic data, password, or entry codes, or presents, exports, imports, issues or promotes them in order to commit any crime defined in this law shall be punished by hard labor for a period not exceeding five years and be issued a fine of no less than five thousand Jordanian Dinars and no more than ten thousand Jordanian Dinars or the equivalent thereof in the legally circulated currency." The article imposes severe penalties on a person for just acquiring devices, programmes or electronic data with the intention of committing any of the offences provided for under the Cybercrime Decree Law. It further prescribes an unduly excessive penalty for any offence, which might be perpetrated by means of these "tools". As such, Article 26 impinges on the general rules of, and the principle of proportionality between, criminalisation and punishment. It also penalises acts which have already been criminalised under the Decree Law, thus imposing more than one penalty for the same offence.

12. According to Article 28 of the Cybercrimes Decree Law, "Any person who creates a website, an application or an electronic account, or who disseminates information on the Internet or an information technology platform with the intention to commit or to entice someone else to commit any offense punishable under any applicable legislation, is subject to twice the punishment stipulated by the relevant law." As opposed to general rules of the Penal Law, this is an overly broad and loosely defined provision. In addition, the Law takes the method used to commit an offence to aggravate the penalty regardless of the nature of the offence in question. Derogating from the Budapest Convention's

approach, Article 28 establishes as cybercrime all the offences provided for under effective regulations.

13. In accordance with Article 30 of the Cybercrimes Decree Law, "If one of the offenses stipulated in this resolution was committed in the name a legal person, the legal person shall be punished by a fine of no less than five thousand Jordanian Dinars and no more than ten thousand Jordanian Dinars. The court may deprive the legal person of their (online???) activity for a maximum period of five years, or to dissolve it without prejudice to the criminal liability of its natural person." The excessively severe penal fines and precautionary measures prescribed by this article, do not take into account the nature and gravity of the offences committed, hence violating the principle of proportionality under the three-part test.

By contrast, Article 36 of the 1960 Penal Law stipulates that for a corporate body to be suspended or dissolved, a crime or misdemeanour with a penalty of at least two years [in prison] should be committed. A final court decision must be in place to prevent/suspend a juridical person from exercising their activity for a certain period of time or to dissolve it. Accordingly, this article needs to be viewed in the same light of blocking websites. In this context, in the aforementioned 2011 joint declaration on freedom of expression and the Internet[3] confirmed that "[m]andatory blocking of entire websites, IP addresses, ports, network protocols or types of uses (such as social networking) is an extreme measure – analogous to banning a newspaper or broadcaster – which can only be justified in accordance with international standards […]".

14. According to Article 31 of the Cybercrime Decree Law, "Anyone that uses an electronic system, a website or an electronic application to bypass the blocking of a website or any other IT platform under the order of this resolution, shall be punished by imprisonment for a period of at least three months or by a fine of no less than five hundred Jordanian Dinars and no more than one thousand Jordanian Dinars or by a combination of both punishments." This is an unjustifiable provision. On the one hand, the blocking of websites *per se* is a violation of relevant international standards. On the other hand, it contravenes the principle of necessity because it implies an unjustified restriction of the right of access to information. For example, blocking certain websites can be used to silence opposition. Against this backdrop, what are the guarantees against the abuse of blocking websites (the first level of the three-part test)? What overriding legitimate interest is to be achieved by this measure (the second level of the three-part test)? Blocking websites renders the right of access to information meaningless and violates relevant international standards. In addition, Article 31 disregards widespread up-to-date technologies and programmes, which can easily bypass blocked websites.

[3] See FN 1

DISCLAIMER
This document is a rough translation written in Arabic, which can be found at:
http://www.alhaq.org/arabic/index.php?option=com_content&view=article&id=868:-2017-&catid=86:2012-05-09-07-29-49&Itemid=201

15. According to Article 32 of the Cybercrime Decree Law, "Service providers commit, as per legal procedure, to the following:

1. At the request of the prosecution or the competent court they shall provide the competent authorities with all necessary data and information that will assist in uncovering the truth.
2. Based on the orders issued by the judicial authorities, and taking into account the procedures stated in Article (40) of this law, they shall block any link, content or application on the Internet.
3. Retain information about the subscriber for at least three years.
4. In accordance with the decision of the competent judge of the court, they shall assist and cooperate with the competent authorities in collecting, recording and retaining information and electronic data."

In addition to breaching relevant international standards, this article gravely violates the right to privacy. In relation to the content, it allows room to infringe upon subscribers' personal information. In his 2017 report to the UN Human Rights Council, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression highlights that "[p]roviders should only be compelled to release user data when ordered by judicial authorities certifying necessity and proportionality to achieve a legitimate objective." (Para. 19).

Hence, Article 32 contradicts the principles of necessity and proportionality. Service providers may not be obligated to retain subscriber information for at least three years on preventive grounds and for the purpose of communications surveillance. To this end, in his 2013 report (A/HRC/23/40) to the UN Human Rights Council, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression says: "states are adopting mandatory data retention laws requiring Internet and telecom service providers […] continuously to collect and preserve communications content and information about users' online activities. Such laws enable the compilation of historical records about individuals' e-mails and messages, locations, interactions with friends and family, etc. […] National data retention laws are invasive and costly, and threaten the rights to privacy and free expression. […] mandatory data retention laws greatly increase the scope of State surveillance, and thus the scope for infringements upon human rights. Databases of communications data become vulnerable to […] accidental disclosure." (Para. 65).

In his 2017 report to the UN Human Rights Council (A/HRC/35/22), the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression also states: "[…] overbroad requests for user data and third party retention of such data […] can have both near and long-term deterrent effects on expression, and should be avoided as a matter of law and policy. At a minimum, States should ensure that surveillance is authorized by an independent, impartial and competent judicial authority certifying that the request is necessary and proportionate to protect a legitimate aim." (Para. 78).

Therefore, the definition of "subscriber information" under Article 1 of the Cybercrime Decree Law needs to be limited to information with regard to the type of communications service used, technical conditions, period of service, subscriber identity, postal or geographical address, telephone number and available payment data based on the service agreement or installation. Subscriber information should also be restricted to data regarding the installation site of the communications service. With a view to protecting and preserving the right to privacy and sanctity of private life, this definition must not include any data on the "content" of the personal information of a subscriber's activity.

Article 32(2) of the Cybercrimes Decree Law provides for the blocking of websites. As explained in Paragraph 8 under the general comments section above, this measure contradicts UN Human Right Council Resolution (A/HRC/32/L.20) which "[c]ondemns unequivocally measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law and calls on all States to refrain from and cease such measures." According to international human rights standards, exceptional cases in which websites can be blocked must take account of the requirements of necessity and proportionality. These standards also require that a final decision be rendered by the competent court. The aforementioned joint declaration confirms that a website may not blocked during the course of preliminary investigation. Such a decision should be applied to more serious crimes, such as organised crime or child pornography.[4]

16. Articles 33 and 34 of the Cybercrime Decree Law give the power to the Public Prosecution or the person it delegates from among officers tasked with judicial duties to search people, places and information technology tools relevant to an offence. The search warrant must be reasoned and may be renewed more than once as long as the justifications for the procedure remain in effect. The Prosecutor may authorise officers tasked with judicial duties or those experts who assist them to have direct access to any information technology tool and conduct the search with the intention of obtaining data and information. The Public Prosecution shall be entitled to access electronic devices, tools, means, data and information related to the offence. The Public Prosecution shall also be entitled to permit the seizure and confiscation of the information system wholly or partly or any other information technology tool which may help uncover the truth.

Although it is an adversary party to penal cases, the Public Prosecution is given powers that fall within the jurisdiction of courts thus violating guarantees of the right to privacy under international standards. The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression states in his 2013 report (A/HRC/23/40) to

[4] See FN 1

DISCLAIMER
This document is a rough translation written in Arabic, which can be found at:
http://www.alhaq.org/arabic/index.php?option=com_content&view=article&id=868:-2017-&catid=86:2012-05-09-07-29-49&Itemid=201

the Human Rights Council that "communications surveillance should be regarded as a highly intrusive act that potentially interferes with the rights to freedom of expression and privacy and threatens the foundations of a democratic society. Legislation must stipulate that State surveillance of communications must only occur under the most exceptional circumstances and exclusively under the supervision of an independent judicial authority. Safeguards must be articulated in law relating to the nature, scope and duration of the possible measures, the grounds required for ordering them […]" (Para. 81). Hence this measure must fall within the jurisdiction of the Judicial Authority.

It should also be noted that according to the Cybercrimes Decree Law, the search warrant issued by the Public Prosecution is indefinite; i.e. it is not limited to a specific period of time and can be conducted in the absence of the accused person which contravenes procedural guarantees. A search is supposed to be strictly exceptional and governed by guarantees to prevent potential abuse. In general, the said articles imply a clear violation of the tests of necessity and proportionality under the respective international standards. They also demonstrate a derogation from the guarantees enshrined in the Penal Procedure Law.

17. In accordance with Article 35 of the Cybercrime Decree Law, "1. The Magistrate's Court may authorize the Public Prosecution to monitor, register and deal with communications and electronic conversations in order to uncover evidence relating to the crime. This authorization is valid for a period of fifteen days and is renewable once, providing the availability of new evidence. 2. The Public Prosecution may order the immediate collection and provision of any data, including communications, electronic information, traffic data or content information that it deems necessary to conduct the investigations. The Public Prosecution shall use the appropriate technical means and may resort to consulting the service providers if necessary."

In reference to communications surveillance, Article 35(1) derogates from the guarantees set forth by Article 51 of the Penal Procedure Law. Accordingly, this power (i.e. communications surveillance) is given to the Attorney General or one of his assistants based on an authorisation from the Magistrate Court judge. A judicial order on communications surveillance must be issued and reasoned by the Magistrate Court judge. However, this applies to specific and not all offences. Article 35(2) also contravenes guarantees enshrined in the Penal Procedure Law. While Article 35(2) provides that this measure can be initiated based on a decision from the Public Prosecution and without a judicial order, relevant international standards prescribe that communications surveillance can only be conducted through judicial authorities.

DISCLAIMER
This document is a rough translation written in Arabic, which can be found at:
http://www.alhaq.org/arabic/index.php?option=com_content&view=article&id=868:-2017-&catid=86:2012-05-09-07-29-49&Itemid=201

Article 35 also neglects the right of individuals to be "notified" of communications surveillance. In this vein, the 2014 International Principles on the Application of Human Rights to Communications Surveillance provide that "[t]hose whose communications are being surveilled should be notified of a decision authorising Communications Surveillance with enough time and information to enable them to challenge the decision […] Delay in notification is only justified if notification would seriously jeopardise the purpose for which the Communications Surveillance is authorised, or there is an imminent risk of danger to human life. The User affected is notified as soon as the risk is lifted. Governments should publish, at a minimum, aggregate information on the number of requests approved and rejected. Communications surveillance must also be subject to public oversight."

This is also highlighted by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression in his 2013 report (A/HRC/23/40) to the Human Rights Council: "Individuals should have a legal right to be notified that they have been subjected to communications surveillance or that their communications data has been accessed by the State. Recognising that advance or concurrent notification might jeopardise the effectiveness of the surveillance, individuals should nevertheless be notified once surveillance has been completed and have the possibility to seek redress in respect of the use of communications surveillance measures in their aftermath" (Para 82).

The test of proportionality must always be maintained. That is, the least intrusive mechanism must be used to achieve the interest to be protected. In other words, if a less invasive mechanism is available and has not been exhausted, communications surveillance should be avoided.

18. Pursuant to Article 37 of the Cybercrimes Decree Law, "1. The competent court may authorize the immediate objection to the content of communications and may record or copy them at the request of the Attorney General or at the request of one of his or her aides. The decision of the court shall include all the elements that would define the communications which are subject to the objection. 2. The duration of the objection specified in paragraph (1) of this Article shall be three months from the date of actual commencement, which may only be extended once." This is a further derogation from the guarantees enshrined in Article 51 of the Penal Procedure Law. These provisions apply to all the offences provided for under the Cybercrimes Decree Law. Unlike the specification made by the Penal Procedure Law, the Cybercrimes Decree Law subjects communications to surveillance without reference to the criterion of gravity. Undermining the guarantees provided by the Penal Procedure Law, Article 37(2) increases the period of communications surveillance to three months, renewable for another 3 month period.

DISCLAIMER
This document is a rough translation written in Arabic, which can be found at:
http://www.alhaq.org/arabic/index.php?option=com_content&view=article&id=868:-2017-&catid=86:2012-05-09-07-29-49&Itemid=201

19. Article 38 of the Cybercrimes Decree Law provides that "any piece of evidence resulting from a means of information technology, information system, information network, website or electronic data and information may not be excluded because of the nature of the evidence." This is an unacceptable interference with the court's conviction when it deals with admissible evidence. It also intervenes in the penal judge's freedom to prove, elicit, determine the weight of, approve or reject evidence in penal cases. Therefore, Article 38 involves a flagrant breach of judicial independence. This is also the case of Article 39 of the Cybercrime Decree Law.

20. According to Article 40 of the Cybercrime Decree Law, "(1) In the event websites hosted within or outside the State post any statements, figures, images, films, propaganda or other material, which may threaten the national security, community safety, public order or public morals, the Investigation and Interdiction Units shall be entitled to submit a report to this effect to the Attorney General or to one of his assistants and request an authorisation to block the website/s or to block some of their links from being displayed. (2) Within 24 hours, the Attorney General or one of his assistants shall file the request for authorisation to the Magistrate Court, together with a note of his opinion. The court shall render its decision, either accepting or rejecting the request on the same day it is filed."

Given the overly broad contexts, of public order, public morals, etc., this Article allows for the blocking of websites within 24 hours at the request of the Attorney General or one of his assistants and based on a decision from the Magistrate Court. As mentioned above, this measure contradicts the 2016 UN Human Right Council Resolution (A/HRC/32/L.20) which condemns calls on states to end measures of intentional prevention or disruption the access to or dissemination of information online. To be applied in extremely exceptional cases, this measure must take account of the requirements of necessity and proportionality. It also requires that a final court decision be rendered to this effect. Such a decision should apply to more serious crimes, such as organised crime or child pornography. In addition to contravening the principles of legality and knowledge of legal norms, vague and loosely defined terms are also contrary to international standards, particularly the framework set by Article 19 of the ICCPR in reference to the right to freedom of expression. Accordingly, Article 40 cannot be in line with international standards.

21. Article 41 of the Cybercrimes Decree Law states that "With exception of the professional obligations provided for in the law, the secrets or requirements of the profession may not be invoked to refrain from providing the information or documents required and which are in accordance with the provisions of the law." This article is neither necessary nor justifiable. Confidentiality in professions, such as in medicine and law, are safeguarded by relevant protective laws. If this article is to be kept,

DISCLAIMER
This document is a rough translation written in Arabic, which can be found at:
http://www.alhaq.org/arabic/index.php?option=com_content&view=article&id=868:-2017-&catid=86:2012-05-09-07-29-49&Itemid=201

confidentiality agreements of any profession must be respected and only disclosed following a judicial order. The word "law" should also be replaced by "legislation" given that professional secrets are regulated by laws, regulations, etc.

22. In accordance with Article 44 of the Cybercrime Decree Law, "[t]he competent authorities shall provide assistance to counterparts in other States for the purposes of mutual legal aid and extradition of criminals in criminal investigations and proceedings associated with the offences set out in this resolution..." This article contradicts Article 28 of the Basic Law, which categorically prohibits the extradition of Palestinians to foreign entities. Trials must be held in Palestine. Also, similar to Article 43, this provision seems to have ignored the extraordinary status of the State of Palestine as a territory under occupation.

23. Article 46 provides that "Any person who commits, participates in, intervenes in or instigates an act using the Internet or any other means of information technology which constitutes an offense under any applicable legislation, shall be liable to the penalty prescribed for the crime in question under that legislation." Contrary to the approach set by the Budapest Convention, this article goes beyond the limits of cybercrime. In the context of the Cybercrimes Decree Law, this provision is irrelevant since it focuses on the "method" used to commit an offence which is irrelevant to the penalty imposed so long the crime has been committed.

24. Pursuant to Article 47 of the Cybercrimes Decree Law, "Anyone who creates a website that aims to promote committing any of the crimes stipulated in the Penal Code or in any of the special laws shall be punished by a provisional imprisonment and by a fine of at least five thousand dinars and no more than ten thousand Jordanian Dinars or the equivalent in the legally circulated currency." Expanding the scope of cybercrime, this article contradicts the approach adopted by the Budapest Convention. It also imposes an excessively severe penalty. Temporary imprisonment is not included in the categories of penalties listed under the Penal Law in force. Furthermore, contrary to this categorisation, Article 47 combines penalties prescribed for misdemeanours and crimes.

25. According to Article 48 of the Cybercrimes Decree Law, "Any person who discloses the confidentiality of the procedures provided for in this resolution, other than in cases authorized by law, shall be punished by imprisonment and by a fine of no less than five hundred Jordanian Dinars and no more than three thousand Jordanian Dinars or by one of the two punishments." This article constitutes a violation of the right to freedom of expression and right of access to information. Essentially, the Cybercrimes Decree Law as a whole does not reference any 'procedures of a secret nature', contravening the principle of legality (there is no crime or punishment except as defined by law). In this case, and for example, any evidence collected by security officers vested with judicial tasks in the context of investigation, at the request of the Public Prosecution (search and

DISCLAIMER
This document is a rough translation written in Arabic, which can be found at:
http://www.alhaq.org/arabic/index.php?option=com_content&view=article&id=868:-2017-&catid=86:2012-05-09-07-29-49&Itemid=201

seizure of information technology tools, data, etc.) could be categorised as secret procedures. This may result in breaching the public right of access to information.

26. Article 50 of the Cybercrimes Decree Law provides that "Any person who deliberately refrains from reporting a crime or who knowingly misrepresents or withholds information shall be punished by imprisonment for a period of no less than six months and by a fine of no less than two hundred Jordanian Dinars and no more than one thousand Jordanian Dinars or alternatively they may be subjected to only one of these two penalties." This article imposes penalties on citizens who refrain from reporting cybercrime. By contrast, penal legislation does not criminalise such an omission. The provision also raises questions about how offences with such overly broad and loosely-defined terms can be reported. Although harsh penalities are prescribed under Article 50, Individual behaviour cannot be assessed based on these terms, nor can the intent of such exceptional legislations and regulations be interpreted.
27. According to Article 51, "If any of the offenses set out in this resolution is committed for the purpose of disturbing public order, endangering the safety and security of the community, endangering the lives of the citizens, preventing or obstructing the exercise of public works by the public authorities or obstructing the provisions of the Constitution, the Basic Law, or with the intention of harming national unity, social peace, contempt of religion or that violate of the rights and freedoms guaranteed by the Constitution or the Basic Law, the penalty shall be hard labor or temporary hard labor."

This article contravenes international standards set forth in Article 19 of ICCPR, relating to the right to freedom of expression, constituting a grave violation, and rendering the right meaningless. As mentioned above, the three-part test used to assess any controls on the right to freedom of expression requires that such controls be clearly, explicitly and unequivocally provided by law. Also, Article 51 contradicts the principles of legality and knowledge of legal norms. Legality stipulates an absolutely clear distinction between criminalisation and punishment. Furthermore, this Article is inappropriate to serve as a penal provision.

In reality, concerned individuals cannot identify the legislator's intent given such loosely defined terms, such as public order, national unity, community safety, etc. In addition to the excessive penalty prescribed (hard labour for life or temporary hard labour) which applies to the Decree Law's provisions and should the crime be committed within the scope of any of the loosely-defined terms set forth.

28. According to Article 52 of the Cybercrime Decree Law, "Anyone who participates by way of agreement, incitement, assistance or interference in committing a felony or a misdemeanor punishable under the provisions of this Decree shall be punished by the same penalties as the main perpetrator." The Cybercrimes Decree Law should not derogate from the general rules of criminal complicity, the penalty of which is set forth under the General Section of the Penal Law. It should be noted that this Article also

provides for excessively harsh penalties which require review – along with penalties prescribed by other provisions under the Cybercrime Decree Law – as mentioned above.

29. Article 54 states: "(1) Without prejudice to the penalties provided for in this resolution and to the good faith of others, the Court shall issue a decision to confiscate the devices, programs or means used to commit of any of the offenses which fall under the jurisdiction of this resolution at the expense of the owner. (2) The court shall issue a decision on how long a business shall remained closed or how long a website shall be blocked that had been involved in a crime." This Article jeopardises judicial independence. It compels a judge to seize the devices, programmes or tools used, as well as to close down a premise and block websites; measures that should be subject to the discretionary power of the court and in accordance with international standards as mentioned previously.

30. The Cybercrimes Law by Decree completely disregards the protection of copyright and intellectual rights, and the criminalisation of pertinent violations. The Budapest Convention highlights these issues, especially given that hacked software is widely available in markets, violating copyright and causing exorbitant losses to manufacturers and developers.

Conclusion

The Law by Decree on Cybercrime No. 16 of 2017 was developed and published without earlier civil society participation and in the absence of the PLC. The Law by Decree involves extensive infringements on the right to freedom of expression, right to privacy and right of access to information. It also substantially contradicts the provisions of the Amended Basic Law and international conventions which the State of Palestine acceded to without reservation, particularly the ICCPR and relevant international standards.

In addition, the Cybercrime Decree Law derogates from the Budapest Convention in terms of the nature and limits of cybercrime. Against this background, Al-Haq demands that the **Law by Decree on Cybercrime No. 16 of 2017 be abolished**. A new version needs to be drafted, taking into consideration comments made by Al-Haq and other civil society organisations, to ensure that it is consistent with the Amended Basic Law, international conventions that Palestine is party to, and the Budapest Convention.