IMPASSE OF CYBER LAWS: IRAQI CASE

[**Issue Number 112 - April 2020**](https://www.lebarmy.gov.lb/en/content/112-d)

**Impasse of Cyber laws: Iraqi Case**  
Prepared By: Tania Nehme  
ABD, Rutgers university

**Introduction**

In a joint letter released on March, 02, 2019, several Iraqi and international human rights and media organizations strongly urged the parliament in Baghdad to withdraw, or make significant critical changes to a controversial internet bill. They stated that: "While we recognize the necessity to legislate on cyber criminality, we argue that should this law be enacted in its current form, it would constitute a serious setback for freedom of expression in Iraq, and would establish a climate of self-censorship in the country".

The signatories of this letter include the Iraq Journalists Right Defense Association, the Iraqi Network for Social Media, the Iraqi Observatory for Human Rights, the International Press Institute, Amnesty International, and Human Rights Watch[[1]](https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case" \l "_ftn1" \o ").

The joint letter collaboratively indicated that the text of the Law on Information Technology Crimes that received its first reading in parliament in January 2019, is almost identical to a previous 2011 bill that was collectively condemned as "out of condition" and withdrawn later. The organizations behind the letter were particularly concerned over articles 3, 4 and 6 which punish vague and imprecise acts that could fall under the right to freedom of expression with life imprisonment and heavy fines, the letter states that the law defines crimes with unclear or subjective terms that, free speech advocates say, can be used by the government to target those exercising rights enshrined in Iraq's constitution. The recent push by Iraq's Media and Communications Commission to pass the law comes months after internet crackdowns that the Iraqi government enacted in response to demonstrations that recently spread throughout Iraq’s central and southern provinces.

The Iraqi government disabled internet service and further restricted access to social media sites nationwide just as protests exploded, something the Ministry of Communications proclaimed was caused by "technical difficulties". "Amnesty International commented on the events stating that "Peaceful protesters, who were fired on by security forces, believe the authorities deliberately disabled internet access as they were unable to share images and videos depicting the abuses"[[2]](https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case" \l "_ftn2" \o ").

It is this joint letter that motivated the writing of this article especially when in today’s political arena people are continuously connected to the outfitted world. Approximately Four and a Half billion people possess an average of 4 electronic devices. This phenomenon has become so complex that even the inventers themselves can’t keep up with its evolution.

Every invention elicits the virtuous and the corrupt. Almost all people’s functional activities orbit around computerized smart devices. Global connectivity has brought about such a rising that the post-net and pre-net worlds are completely different. People’s existence, priorities, and values have changed, and so, have their problems.

**Online Activities**

With the increasing popularity of online activities, the rate of online crimes has also increased exponentially. While the extent and impact of these crimes vary greatly from one country to another, it has become an international peril. From crimes like cyber bullying to cyber terrorism, these new age phenomena have evolved and are evolving constantly.

Cybercrimes are still far from being explicitly defined. While most nation-states have laws in place to deal with such issues, the underlying crime itself varies from case to case despite the fact that cyber activities are not governed by topographical borders. This fact brands such crimes all the more perplexing and intricate.

Cyberspace, digital technology and devices have become the foundation upon which communities and businesses are built, and digital usage has become indicator and a measurement of development. That is why international societies recognize a strong sense of urgency to develop global cyber capacities to address the risks to cyberspace covering both the known, unknown and the unanticipated aspects of this phenomenon. With more accessibility, anonymity and convenience, the cyberspace allowed new forms of crimes to emerge, while also allowing traditional crimes to be committed in an easier and faster way. There has become a great need for new cyber capacities that deal with the new cyber territory. These include but are not limited to daily practice, national policy, local expertise, and both local and international cooperation, rapid crisis response, and long-term development programming. Thus, the constructing and developing of global cyber measurements, global awareness and resilience could enable citizens, organizations and nations to take better advantage of cyberspace opportunities. There could be difficulties to achieve that due to differences in culture, law, governance, organizational structures, and pace of cyber development, and thus capacity building efforts will need to be tailored to the needs of nations according to their needs for development[[3]](https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case" \l "_ftn3" \o ").

Selecting the Iraqi state as a case to gaze at the current efforts and measures that have been taken to deal with this issue is not enough if constrained by time and dates, because the internet is at a constant state of evolution. Law makers and law enforcements in Iraq cannot keep up with the rapid developments. As it stands at this point in time, Iraq's internet sector is currently unregulated, placing it among the most vulnerable. The current political and security situation in Iraq means that further work is necessary to develop the legal, technical, organizational, and capacity building fundamentals to provide comprehensive cybersecurity for its citizens, businesses, and the fragile state as is.

Moreover, dealing with the Iraqi case is not simple because reliable data on the types of cybercrime in Iraq is insufficient and rarely published by the Iraqi government. However, reports released by non-governmental organizations expose the most common types of cybercrime in Iraq, which have significantly increased over the last seven years.

The vast majority of cybercrime in Iraq is conducted via social media platforms, primarily on Facebook, and against persons rather than businesses or governments. The most common cyber attacks involve internet fraud, identity theft, child pornography, cyber-stalking, cyber-blackmail, copyright infringement, satellite piracy, and cyber terrorism.

At an early stage of cybercrime in Iraq a draft was prepared by Iraqi Information Crimes Law and later proposed by the Presidential Council of Iraq in 2011. The draft law was intended to regulate the use of information networks, computers, and other electronic devices and systems. The proposed legislation was deemed by International and local Human rights organizations as violating international standards protecting due process, freedom of speech, and freedom of association. On 6 February 2013 following these strong objections, as well as a decisive letter by the Iraqi Council of Representatives' Culture and Media Committee addressed to the head of the Council, the Iraqi Council of Representatives revoked and discarded the draft law[[4]](https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case" \l "_ftn4" \o ").

Iraq does not currently have any specific legislation on cybercrime in place. In the absence of such legislation, the judiciary must apply the provisions of the Iraqi Civil Code No. 40 of 1951 (the "Civil Code") and the Iraqi Penal Code No. 111 of 1969 (the "Penal Code"), in addition to sector-specific laws (e.g. the Banking Law of 2004, and Communications and Media Commission Law CPA Order 65 of 2004), to cases involving cybercrime. Furthermore, Iraq does not currently have any specific data protection legislation in place and privacy protection. The Civil Code remains largely undeveloped. There is reference to a "right to personal privacy" in the Iraqi Constitution of 2005, but guidance with respect to this right is unavailable, and it remains undefined in legislation.

The Internet is a unique and outstanding domain, and thus, laws that regulate other forms of media cannot always effectively govern this medium, and attempting to have them do so may create inconsistency and ambiguity in application. Regulatory approaches need to be tailored specifically for the internet and the criminalization of e-crimes. While the Penal Code and Civil Code, in addition to the sector-specific laws dealing with e-transactions, serve as a step towards the establishment of cybersecurity, it is hoped that the Iraqi legislature will adopt articles specifically relating to cybercrime. Specific and extensive cybercrime legislation will provide judicial consistency on the subject as well as facilitate the enforcement of the law[[5]](https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case" \l "_ftn5" \o ").

**Fitting Laws for Cybercrime**

One cannot but acknowledge the needs for cyber-space in all societies, however, we should recognize that cybercrimes as its monster child. Lawmakers have constantly been puzzled if the construction of laws against cybercrime possible? If so, how difficult of a task would it be? Might it lead to more problems than solutions?

In general, cybercrime is a term for any illegal activity that employs a computer as its primary resource. The U.S. Department of Justice goes furthermore and incorporates in the definition "any illegal activity that utilizes a computer for the deformation of evidence". However, there are a number of controversial issues surrounding the definition of cybercrime.

Cybercrime can be far reaching with long-term effects, from the impact on organizations from the theft of intellectual property or business secrets to the consequence’s identity theft can have on an individual, including credit standing and loss of personal resources.

Responding to cybercrime in Iraq specifically is even more challenging because the economics in a politically destabilized country favor the criminals. With just a laptop, a single individual can wreak havoc on individuals and organizations with minimal cost and little risk of being caught. The only solution that Iraq could provide is to solicit for more advanced technologies and protective measures. This will eventually deter immoral conduct, help security officers catch and prosecute perpetrators and level what has become an unbalanced competitive arena. In the meantime, it is imperative that the Iraqi government establishes an educational institution to enlighten all digital users to practice basic cybersecurity hygiene to increase their own protection and improve cybersecurity overall, especially when appropriate laws in Iraq are lacking.

It is estimated that roughly 80 percent of exploitable vulnerabilities in cyberspace are the direct result of poor or nonexistent cyber hygiene among most Iraqis. While it is also important to address the remaining 20 percent of more-sophisticated intrusions, advanced persistent threats, distributed denial of service attacks, destructive malware and the growing challenge of ransom-ware, raising the bar for basic cyber hygiene will improve cyber security protection profile and reduce the threat from cybercrime[[6]](https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case" \l "_ftn6" \o ").

**Law and Cybercrime Activities**

One of the problems is the different opinions the majority of the law enforcers have on whether certain cyber activities should be considered as cybercrimes or even crimes of norms in general. The ability to draw a line between what is acceptable and what isn’t is the dilemma they deal with. For example, should cat-fishing (the act of baiting individual/s into a relationship through the creation of a fictional online persona) someone online be considered as a crime? In the offline world, giving someone a fake name isn’t considered a national crime. However in the online world, due to lack of physical contact, it could be considered as pedophilia and child pornography for example, if the cat-fisher is a 40 year old male who infiltrates himself into a conversation with an 11 year old girl by posing as her peer in order to freely converse with her and eventually obtain unethical photos of her after gaining her trust. Moreover, whose fault is it? The 40-year-old male who is taking advantage of the anonymity of the internet, or the vulnerable girl who at some point willingly gives her "peer" photos of herself? However, when it comes down to it, cybercrimes fall under four major categories: hacking, soliciting and abuse, copyright theft and piracy, and illegal trade.

Due to its complexity, cybercrimes face even further complicated issues. The first is the lack of reporting and resources. This is due to the fact that most law enforcement offices are not suitably trained to deal with cybercrime issues and/or lack a suitable cyber forensic department.

Moreover, at times, the perpetrator is located, not only in a different country, but sometimes in a completely different continent. Thus, law enforcers are unable to execute their jurisdictional authority on the criminal perpetrator even if they did find out their identity and location.

The second issue is the emergence of E-cash, such as prepaid cards, mobile payments, internet payment services, and crypto currency. Any economically motivated crime can, not only harm individuals, but could also harm a nation or even reach global harm due to its boundary-less reach.

The third issue is the lack of uniform international laws, due to a combination of cultural differences, political differences, jurisprudential inconsistency and diversity, and state sovereignty. Even though there exists a lack of uniform international laws on the subject matter, there are certain international efforts that have attempted to deal with this issue. First, we look at the Global Forum on Cyber Space expertise (GFCE). This Global Forum is a platform for countries, international organizations and private companies to exchange best practices and expertise on cyber capacity building. The aim is to identify successful policies, practices and ideas and multiply these on a global level. With partners from NGOs, the tech community and academia GFCE members developed practical initiatives to build cyber capacity. However, this forum exists for consultation purposes and exercises no legal action internationally[[7]](https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case" \l "_ftn7" \o "). Then we look at the United Nations and their initiatives towards cyber security and development. The United Nations developed a UN Group of Governmental Experts (UN GGE). This group was developed five times in five different meetings; however they failed to come to an international consensus and thus eventually stopped its initiative in creating international laws. After that, came the OECD (The Organization for Economic Co-operation and Development), and the Select Committee of Experts on Computer Related Crime of the Council of Europe. However, this organization, similar to the GFCE, was only created for consultation purposes for the Council of Europe. Finally, we look at the Budapest Convention. This convention is also European based; its main purpose is to harmonize national cyber laws, improve investigative techniques, and increase cooperation among nations. The convention consists of 63 parties and 67 signatories, which include Canada, Japan, the United States, South Africa and the council of EU states, Australia, Dominican Republic, Israel, Japan, Mauritius, Panama, and Sri Lanka. The reason behind the successes of this convention in exercising legal action is due to the fact that it allows the participatory states to exercise their sovereignty during arrest and allows the state to take the criminal to trial, if found in their territory, on the condition that these participatory states allow foreign states to send investigation claims and petitions for warrants (search, arrest…). Despite its successes, this convention also has its failures. After studies were made, it had been concluded that US involvement hindered the unification of domestic laws and untimely lead to discrepancies in sentencing the cybercrime cases of this convention. Moreover, there are not enough Signatory/Ratifying states for this convention to have global reach and make all global states bound by its laws[[8]](https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case" \l "_ftn8" \o ").

**Cybercrime in Iraq**

Iraq, like any other underdeveloped country, is not immune to cybercrimes. As stated previously in this article, in order for Iraq to tackle cybercrime, a draft of Iraqi Information Crimes Law was proposed by the Presidential Council of Iraq. The draft was divided into four chapters: definitions and goals; punitive provisions; procedures for collecting evidence, investigation and trial; general regulations and conclusion. The draft first surfaced in mid-2011. Although its provenance remains uncertain, it was believed to have been drafted by the Prime Minister’s Office. The proposed law did not go through the legal committee in parliament before it was put to the vote, which raised the question of its legibility. Moreover, it was leaked while in draft form and translated into English by IREX, an international media freedom NGO, and was then distributed to local and international organizations for scrutiny and analysis. Several Human Rights Groups and Activists called on the Iraqi government to refrain from proposing the law to vote, to amend its controversial and loose articles, and make them more precise and specific to be up to standard and in accordance with international law. It was said to have been contravening the Charter of the United Nations, the Universal Declaration of Human Rights of 1948, and the International Covenant on Civil and Political Rights of 1976"[[9]](https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case" \l "_ftn9" \o ").

Article 19 of the International Covenant provides that: "Everyone has the right to hold opinions without interference, and everyone has the right to freedom of expression, including the right to seek, receive and impart information and ideas of all kinds, regardless of frontiers, whether in written or printed form in the form of art or by any other means of his choice." One would assume that the creation of laws would be beneficial to a country especially in the realms of cyber security matters, thus, what were the issues faced?

The main concerns stemmed from the understanding that the law showed extreme restrictions and severe penalties that strengthen the dictatorship, violation, and repression of public rights. The law included clauses imposing fines and penalties, and the right to interpret texts written on the web by citizens according to specific intention, which makes any publication/ information published via social media sites questionable and could be held accountable for, and subject to prison penalties and financial fines. The law of informatics cybercrimes included 23 articles under various paragraphs, all of which provided penalties ranging from thirty years of imprisonment to fines that reach up to 50 million Iraqi dinars. The law also suggested that any computer or set of electronic or connected devices, data, software, systems and Internet services may be subjected to surveillance. There is also the authority to open programs and messages stored in any device if there is suspicion of use or misleading and unrealistic facts. This is included under the reasoning that any information they gather could "compromise the national security and independence of the country"[[10]](https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case" \l "_ftn10" \o ").

For example, Article 2 of the law states that: "This law is intended to provide legal protection for the legitimate use of the computer and the Internet and to punish perpetrators of acts that constitute an infringement of the natural or moral rights of its users and prevent its misuse in committing computer crimes".However, the loose wording of several articles of the law makes them ambiguous and severe penalties that are not proportionate to the type of violations will lead to the confiscation of public freedoms, especially freedom of expression on the Internet. Thus, Human Rights Activists feared the law will be used to target Internet activists and bloggers for their peaceful activities.

**Article 3 states:** "The following shall be punishable by life imprisonment and a fine of no less than 25 million dinars (approximately US$. 21,000) and no more than 50 million dinars (approximately US$. 42,000) to anyone who intentionally uses computers and the Internet for the purpose of committing one of the following acts:

1- To prejudice the independence, unity, integrity or economic, political, military or security interests of the country;

2- To engage, negotiate, promote, contract or deal with an enemy in any way with a view to destabilizing security and public order or endangering the country".

The text of this article undoubtedly raises real risks due to its broad nature and ambiguity, which means the law can be easily used to target human rights defenders and other activists as well as opponents of government policies or leaders of peaceful protests who are active on the Internet because they want to defend the civil and human rights of their fellow citizens.

**Article 4 states:** A person shall be sentenced to life imprisonment and a fine of no less than 25 million dinars (approximately US$. 21,000) and no more than 50 million dinars (approximately US$. 42,000), to anyone who has established or managed a website with the intention of committing one of the following acts:

1- To carry out terrorist operations under false names or to facilitate contact with leaders and members of terrorist groups.

2- To promote terrorist acts and ideas.

Without a clear and explicit definition of terrorism, it would be easy to use this law to liquidate the resources of political opponents and other activists.

**Article 6 states:** Anyone who uses computers and the Internet for the purpose of committing one of the following acts shall be punished with life imprisonment and a fine of no less than 25 million dinars (approximately US$ 21,000) and no more than 50 million dinars (approximately US$. 42,000):

1- To provoke, threaten or condone armed insurrection, provoke sectarian strife, disturb the security and public order, or harm the reputation of the country.

2- To publish or broadcast false or misleading facts with the intention of weakening confidence in the electronic financial system, electronic commercial and financial papers and the like, or harming the national economy and the financial confidence of the state.

The loose wording of the article includes many undefined terms that could ultimately be used to trap Internet activists, opponents of government policies or leaders of peaceful protests under the guise of inciting sedition, undermining security and public order, or abusing the reputation of the country[[11]](https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case" \l "_ftn11" \o "). It might also target those who are working on exposing financial corruption in the governmental and private banks.

**Article 18 states:** A penalty of imprisonment or a fine of no less than 5 million dinars (US$ 4200) and no more than 10 million dinars (US$. 8400) shall be imposed on those who: "Refrain from providing information or data to the judicial or administrative authorities.

This article truly threatens the freedom of the press, as it gives the right not only to the judiciary but also to the government authorities, including the security services, to force activists, journalists and citizen journalists or even ordinary citizens to provide all information and data requested in deliberate violation of their right to privacy and to protect their sources of information.

**Article 21** includes another broad and vague addition to the proposed law, which states the following: Thirdly, a penalty of imprisonment for a period of no less than one year and a fine of no less than 2 million dinars (approximately US$. 1680) and no more than 5 million dinars (approximately US$. 4200) shall be imposed on anyone who violates any religious, moral, family or social principles or values or privacy of private life through the Internet or computers in any form or shape.

**Article** **23** unlawfully imposes collective punishment on Internet activists, as well as suppliers and sellers of computers, as it states the following: A term of no less than 1 year and no more than 2 years along with a fine of no less than 3 million dinars (approximately US$. 2520) and no more than 5 million dinars (approximately US$. 4200) shall be imposed on any person who has intentionally produced, sold, imported or distributed any of the devices, tools, computer programs, passwords or access codes that led to the commission of any of the crimes provided for in this Law.

**Article** **24** sets forth the investigation procedures of the current criminal bodies, as it states that: The investigative authorities shall carry out the investigation procedures and collect evidence and request its proper sources for the crimes as provided for in this law.

This means that whoever is tasked to collect evidence and investigate the cybercrimes are non-specialized entities. The law does not even suggest establishing a competent and skilled private law enforcement team responsible for gathering evidence and investigating these crimes. This law also contradicts the Iraqi Constitution adopted in 2005, in particular articles 15, 17, 37, 38, 39, 40, 41 and **Article 42**, all of which affirmed the right of citizens to freedom, including personal privacy, freedom of information, freedom of expression by all means, freedom of assembly and peaceful demonstration, freedom of association and political parties, freedom of communication, postal, telegraphic, telephone and electronic correspondence, and freedom from censorship, wiretapping or disclosure of personal information. In addition to all that, **Article** **46** of the Iraqi Constitution has expressly stated that "the exercise of any of the rights and freedoms set forth in this Constitution shall not be limited or restricted except by law or on its basis, provided that such limitation and restriction shall not affect the essence of the right or freedom". This constitutes a blatant contradiction between the spirit of this article of the Constitution and the application of the Cybercrime Law that restricts the freedom of citizens on the Internet. The above-mentioned matter triggered outside interventions[[12]](https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case" \l "_ftn12" \o ").

**Applying Existing Legislation**

As noted above, the most common cybercrimes in Iraq are internet fraud, identity theft, child pornography, cyber-stalking, cyber-blackmail, copyright infringement, satellite piracy, and cyber terrorism. The Penal Code broadly addresses the criminal nature of these cybercrimes, but fails to adequately incorporate their cyber property.

Any person who is convicted of a cybercrime involving violence, sexual exploitation, threats, or manipulation may be penalized under Article 369 and 396 of the Penal Code:

Under Article 369 the penalty is imprisonment with a maximum term of 4 years (eighteen years if the victim is younger than eighteen years of age) on any person who assaults another using force, or threatens, manipulates or violates in any way the decency of another male or female, or initiates such violation.

Similarly, Article 396 of the Penal Code imposes a maximum term of imprisonment of 7 years on any person who sexually assaults a man or woman or attempts to do so without his or her consent and with the use of force, deception or other means. The penalty for offences against victims under 18 years of age is imprisonment for a term not exceeding 10 years.

In addition to the above, any person who is convicted of a cybercrime involving identity theft, internet fraud, blackmail or other relevant crimes may be penalized by detention under Article 456 of the Penal Code. Any person who is convicted of a cybercrime involving copyright infringement may be penalized under Article 45 of the Copyright Law. Legal relief available to the copyright owner under Article 45 includes:

• Injunctions to order the infringer to cease infringing activities;

• Confiscation of the original and copies and materials used to manufacture infringing copies;

• Confiscation of the proceeds of the infringement.

Any person who is convicted of cyber-terrorism may be penalized under the Anti-Terrorism Law No. 13 of 2005. The above provisions are in addition to the civil rights of harmed persons to file claims for damages caused to them by virtue of said violations, in accordance with the Civil Code.

**Transnational Reaction to Restricting Freedoms**

The following recommendations were sent out by the United Nations and other NGOs to the Presidential Council of Iraq:

1- The right to freedom of expression and the right to freedom of information should be expressly guaranteed in the Iraqi legal framework.

2- The Draft Law should incorporate positive examples of technology’s role in enhancing enjoyment of fundamental human rights.

3- 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.

4- Proportionality should be established between penalties and crimes.

5- 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.

6- To use more specific terms, rather than ambiguous ones, to leave no room for loopholes.

On 22 January, 2013 the long-running campaign against the draft of Iraqi Cybercrimes law brought about results. The Iraqi Speaker of the House approved a request to the Parliamentary Committee for Media and Culture to permanently revoke the proposed legislation. The decision was considered as a victory for Iraqi civil society activists after months of public protests and intense negotiations with policymakers[[13]](https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case" \l "_ftn13" \o ").

Currently, Iraq’s internet sector is unregulated, placing it among the freest globally, but also amongst the most vulnerable. The current political and security situation in Iraq means that further work is necessary to develop the legal, technical, organizational, and capacity building fundamentals to provide comprehensive cyber security for its citizens, businesses, and the state.

Data on the types of cybercrimes in Iraq is also scarce, and rarely published by the Iraqi government. 2013 was the earliest report released by the Iraqi government making all their findings severely outdated. Iraq does not currently have any specific measures on cybercrime in order. In the absence of specific legislation, the judiciary must apply the provisions of the Iraqi Civil Code No. 40 of 1951 (the "Civil Code") and the Iraqi Penal Code No. 111 of 1969 (the "Penal Code"), in addition to sector-specific laws (e.g. the Banking Law of 2004, and Communications and Media Commission Law CPA Order 65 of 2004), to cases involving cybercrime. Furthermore, Iraq does not currently have any specific data protection legislation in place and privacy protection under the Civil Code remains largely undeveloped. There is reference to a "right to personal privacy" in the Iraqi Constitution of 2005, but guidance with respect to this right is unavailable, and it remains undefined in legislation[[14]](https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case" \l "_ftn14" \o ").

As mentioned previously, with the emergence of  new types of cyberspace crimes, other traditional crimes took place in new platforms. Thus, Iraq penalizes these crimes according to existing legislation. The Penal Code broadly addresses the criminal nature of these cybercrimes, but fails to adequately incorporate their cyber property.

The Internet is a unique domain. Laws that regulate other forms of media cannot always effectively govern this medium, and attempting to have them do so may create inconsistency and ambiguity in application. Regulatory approaches need to be tailored specifically for the internet and the criminalization of e-crimes. While the Penal Code and Civil Code, in addition to the sector-specific laws dealing with e-transactions, serve as a step towards the establishment of cyber security, it is hoped that the Iraqi legislature will adopt articles specifically relating to cybercrime. Specific and extensive cybercrime legislation will provide judicial consistency on the subject as well as facilitate the enforcement of the law.

New research on emerging cybercrimes and most common types of cybercrimes in Iraq is a must. This step would then create a clear map that allows law enforcers to be steered in the right trajectory of what to focus on the most, to provide concerned officials with the best and most adequate training programs. Not doing so would waste time of institutions, resources, energy and effort in the wrong places. Another possible solution would be to either sign or ratify the Budapest Convention on Cybercrime[[15]](https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case" \l "_ftn15" \o "). I won’t go into detail about this only because in my opinion this option is farfetched. This is so because of the USA's heavy involvement in this convention. Thus, the final solution would be to write a new draft of laws concerning cybercrimes while keeping in mind past mistakes and taking into consideration new findings and statistical data.

**Conclusion**

Current debates around cyber security in Iraq raise various issues, such as how to frame the policy discussion and how to differentiate it from cyber surveillance concerns. In order to create a balanced and constructive multi-stakeholder dialogue and action to deal with cyber security threats, there is an imperative need to ensure that human rights lie at the core of a balanced and comprehensive view of cyber security.

Cyber security has over Four Hundred cyber security related concepts that were catalogued by a variety of institutions and organizations, including governments, businesses, international organizations, the technical community, and civil society. Cyber security threats affect the entire Internet ecosystem, including the physical infrastructure, software/hardware, and applications not only in Iraq but worldwide. It relates to the protection of information that people share and maintain online and in cyberspace, including communications, financial information, medical records, proprietary data, and more. Some of these threats have far more concerning impacts than shutting down a website or accessing data. It can have serious impacts on people's lives, from advocates, to journalists, to consumers.

Cybercrimes have signified a new and rapid growing crime type in Iraq in recent years. Available statistics illustrate that kidnaps scores over Face-book are the most significant. Suffice to mention that the following cybercrimes are on the increase in politically and economically devastated Iraq. Increase by percent: Satellite Piracy 20%; Child Pornography is about 14%; Internet Fraud 33%; Computer Hacking 7%; Information Hacking 15%; Copyright Theft 11%; Child Abuse 27%; Copyright Violation 24%; Satelite Piracy 20%; Infringement of Computer Systems 13%; Internet Fraud 10%; Privacy 6%[[16]](https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case" \l "_ftn16" \o ").

The numbers of arrested persons in Iraq have increased as follows: DVD & Drives 7%; Routers 6%. USB 10%; Wireless Cameras 11%; Printed Badges 15%; SIM Cards 35%; Mobile Phone Memory Cards 10%; and Laptop Computers 6%.

With this perspective in mind, Public Knowledge characterizes cyber security as the preservation through policy, law, technology, best practices, cooperation, and education, both in the civilian and military fields. The availability of laws that protects confidentiality and integrity of information and its underlying infrastructure are required, so as to preserve the security of networks and ultimately people both online as offline.

Cybersecurity laws and policies have a direct impact on human rights, particularly the right to privacy, freedom of expression, and the free flow of information. Policymakers have created several national policies with the intention of protecting the Internet and other information communication technologies (ICTs) systems against malicious actors. However, many of these policies are overly broad and ill-defined, and lack clear checks and balances or other democratic accountability mechanisms, which can lead to human rights abuses and can stifle innovation. For example, extreme cybersecurity laws as in the case of Iraq can be used to censor dissidents, monitor communications, and criminalize online users for expressing their views.

Cybersecurity should not be totally the responsibility of the Iraqi legislature; it is a shared responsibility and requires the attention of a broad range of stakeholders. It requires an effective public/private partnership that incorporates businesses and institutions of all sizes along with national, state, local, tribal and territorial agencies to produce successful outcomes in identifying and addressing threats, vulnerabilities and overall risk in cyberspace. Individual consumers also have a role, and adding cybersecurity to K-12 as well as higher education curriculums will help raise awareness for all users. Teaching users how to protect themselves better is a necessary component to any strategy. A framework addressing cybercrime should include these strategies.

It is worth to indicate that in various cases the use of computer is not altering the basic nature of the crime. For example, a corruption remains a corruption, despite the amount of funds sent electronically on cybercrime and even with the fact that the use of the Internet influences the level of a crime. The Internet is thus attractive to the scientific-expertise criminals since it gives them the possibility to find an array of victims, extend their line of work and then the ability to alter the characteristics. Significantly, they can work from anywhere in the world, making their crime more complex, due to the different framework and the global procedures that must be followed to understand them and convict them.

**Bibliography**

- David Brystowski, "European Certificate on Cybercrime and Eevidence cybercrime Program", 2017.

- United Nations International Crime and Justice Research Institute, 2013.

- Markopoulou P, "The convention on cybercrime", Intellectum, 2018.

- Papanis E., "Research about the Face book", http://www.dart.gov.gr/data/2010.

- Christdoulaki M and Fragopoulou P, "Reporting illegal internet content", International Management and Computer Security, volume 18, pp. 54–65, 2010.  David Brystowski, "European Certificate on Cybercrime and Eevidence cybercrime Program", 2017.

- United Nations International Crime and Justice Research Institute, 2013.

- Markopoulou P, "The convention on cybercrime", Intellectum, 2018.

- Papanis E., "Research about the Face book", http://www.dart.gov.gr/data/2010.

- Christdoulaki M and Fragopoulou P, "Reporting illegal internet content", International Management and Computer Security, volume 18, pp. 54–65, 2010.

- Brysk, Alison. Global Good Samaritans: Human Rights as Foreign Policy. Oxford University Press, USA, 2019.

- Brysk, Alison, and Austin Choi-Fitzpatrick, eds. From Human Trafficking to Human Rights: Reframing Contemporary Slavery. University of Pennsylvania Press, 2018.

- Butler, Clark, ed. Child Rights: The Movement, International Law, and Opposition. Purdue University Press, 2016.

- Calhoun, Craig. Nations Matter: Culture, History and the Cosmopolitan Dream. Third ed. Routledge, 2017.

- Cassese, The Late Antonio. Realizing Utopia: The Future of International Law. Oxford University Press, USA, 2019.

- Coomans, F., and Menno Tjeerd Kamminga. Extraterritorial Application of Human Rights Treaties. Intersentia nv, 2014.

- Crawford, James. The Future of UN Human Rights Treaty Monitoring. Cambridge University Press, 2015.

- Crawford, James, and Martti Koskenniemi, eds. The Cambridge Companion to International Law. Cambridge University Press, 2018.

- Dembour, Marie-Bénédicte. Who Believes in Human Rights? Reflections on the European Convention. 1st ed. Cambridge University Press, 2016.

- Dembour, Marie-Bénédicte, and Tobias Kelly, eds. Paths to International Justice: Social and Legal Perspectives. Third ed. Cambridge University Press, 2017.

- Douzinas, Costas. Human Rights and Empire: The Political Philosophy of Cosmopolitanism. New edition. Routledge-Cavendish, 2017.

- Egan, Suzanne. The UN Human Rights Treaty System: Law and Procedure. Bloomsbury Professional, 2016.

- Fassin, Didier, and Mariella Pandolfi, eds. Contemporary States of Emergency: The Politics of Military and Humanitarian Interventions. Zone Books, 2015.

- Freedman, Rosa. The United Nations Human Rights Council: A Critique and Early Assessment. Routledge, 2018.

- Freeman, Marsha A., Christine Chinkin, and Beate Rudolf. The UN Convention on the Elimination of All Forms of Discrimination Against Women: A Commentary. Oxford University Press, USA, 2012.

- Garsten, Christina, and Monica Lindh De Montoya, eds. Transparency in a New Global Order: Unveiling Organizational Visions. Edward Elgar Pub, 2008.

- Gearty, Conor. Liberty and Security. Polity Press, 2013.

- Gearty, Conor, and Costas Douzinas, eds. The Cambridge Companion to Human Rights Law. Cambridge University Press, 2012.

- Glasius, Marlies. "Do International Criminal Courts Require Democratic Legitimacy?" European Journal of International Law 23, no. 1 (February 1, 2012): 43–66. doi:10.1093/ejil/chr104.

- Goodale, Mark, ed. Human Rights at the Crossroads. Oxford University Press, USA, 2012.

- Goodhart, Michael, ed. Human Rights: Politics and Practice. Oxford University Press, USA, 2009.

- Sattar J. Aboud, "An Overview of Cybercrime in Iraq", the Research Bulletin of Jordan ACM, Volume II (II), pp. 31-34, 2012.

- Cybercrime Legislation in Iraq, by Haydar Jawad - Senior Associate - Corporate / Mergers & Acquisitions. Aro Omar. Erbil, Iraq. Published: September 2017.

- IJSER International Journal of Scientific & Engineering Research, Volume 5, Issue 3, March-2014 425 ISSN 2229-5518 IJSER © 2014. http://www.ijser.org Norton cybercrime report, Symantec, Technical Report, 2019.

[[1]](https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case" \l "_ftnref1" \o ")-  Amnesty international; Iraq: Draconian cybercrimes law threatens freedom of expression, 1 March 2019, 13:19.

[[2]](https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case" \l "_ftnref2" \o ")-  Netblocks: Network data from the NetBlocks internet observatory show that internet access has been cut across much of Iraq as of 21:00 UTC, Monday 4 November 2019 (00:00 Baghdad time, 5 November 2019).

[[3]](https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case" \l "_ftnref3" \o ")-  Norton cybercrime report, Symantec, Technical Report, 2013.

[[4]](https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case" \l "_ftnref4" \o ")-  David Brystowski, "European Certificate on Cybercrime and Eevidence cybercrime Program", 2017.

[[5]](https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case" \l "_ftnref5" \o ")-  Skyline International, Report on Iraq, 2019.

[[6]](https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case" \l "_ftnref6" \o ")-  IJSER International Journal of Scientific & Engineering Research, Volume 5, Issue 3, March-2014 425 ISSN 2229-5518 IJSER © 2014 http://www.ijser.org.

[[7]](https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case" \l "_ftnref7" \o ")-  IJSER International Journal of Scientific & Engineering Research, Volume 5, Issue 3, March-2014 425 ISSN 2229-5518 IJSER © 2014 http://www.ijser.org.

[[8]](https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case" \l "_ftnref8" \o ")-  Norton cybercrime report, Symantec, Technical Report, 2019.

[[9]](https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case" \l "_ftnref9" \o ")-  Cybercrime Legislation in Iraq, by Haydar Jawad - Senior Associate - Corporate / Mergers & Acquisitions. Aro Omar. Erbil, Iraq. Published: September 2017.

[[10]](https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case" \l "_ftnref10" \o ")- Cybercrime Legislation in Iraq, by Haydar Jawad - Senior Associate - Corporate / Mergers & Acquisitions. Aro Omar. Erbil, Iraq. Published: September 2017.

[[11]](https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case" \l "_ftnref11" \o ")- IJSER International Journal of Scientific & Engineering Research, Volume 5, Issue 3, March-2014 425 ISSN 2229-5518 IJSER © 2014 http://www.ijser.org.

[[12]](https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case" \l "_ftnref12" \o ")- Cassese, The Late Antonio. Realizing Utopia: The Future of International Law. Oxford University Press, USA, 2019. Freedman, Rosa. The United Nations Human Rights Council: A Critique and Early Assessment. Routledge, 2018.

[[13]](https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case" \l "_ftnref13" \o ")- Crawford, James, and Martti Koskenniemi, eds. The Cambridge Companion to International Law. Cambridge University Press, 2018.

[[14]](https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case" \l "_ftnref14" \o ")- Crawford, James, and Martti Koskenniemi, eds. The Cambridge Companion to International Law. Cambridge University Press, 2018.

      Dembour, Marie-Bénédicte. Who Believes in Human Rights? Reflections on the European Convention. 1st ed. Cambridge University Press, 2016.

[[15]](https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case" \l "_ftnref15" \o ")- Freedman, Rosa. The United Nations Human Rights Council: A Critique and Early Assessment. Routledge, 2018.

[[16]](https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case" \l "_ftnref16" \o ")- http://www.ijser.org Norton cybercrime report, Symantec, Technical Report, 2019.

**مأزق قانون الانترنت: القضية العراقية**

لا يوجد لدى العراق حاليًا أي تشريع محدد بشأن الجرائم الإلكترونية. فقد ظهرت المسودة التي صيغت لأول مرة في منتصف العام ٢٠١١، ولكنها لم تمر باللجنة القانونية في البرلمان قبل طرحها للتصويت، الأمر الذي أثار مسألة مدى أهليتها بعد اعتراضات قوية في ٦ فبراير ٢٠١٣، وأيضًا الرسالة الحاسمة من لجنة الثقافة والإعلام التابعة لمجلس النواب العراقي والموجهة إلى رئيس المجلس، دفع بالمجلس إلى إلغاء مشروع القانون وتجاهله.

في غياب تشريع محدد للجريمة الإلكترونية، يجب على القضاء تطبيق أحكام القانون المدني العراقي رقم ٤٠ من العام ١٩٥١، وقانون العقوبات العراقي رقم ١١١ من العام ١٩٦٩ بالإضافة إلى القوانين الخاصة بالقطاع (مثل قانون البنوك من العام ٢٠٠٤، قانون لجنة الاتصالات والإعلام وقرار سلطة الائتلاف المؤقتة رقم ٦٥ من العام ٢٠٠٤)، في القضايا المتعلقة بالجرائم الإلكترونية. علاوة على ذلك، لا يوجد لدى العراق حاليًا أي تشريع محدد لحماية الخصوصية وتشريع مطبّق لحماية البيانات. لا يزال القانون المدني غير متطور إلى حد كبير. ففي الدستور العراقي من العام ٢٠٠٥، هناك إشارة إلى "الحق في الخصوصية الشخصية"، ولكن التوجيه في ما يتعلق بهذا الحق غير متوافر، وغير محدد في التشريع.

إن اختيار الدولة العراقية كحالةٍ للنظر في الجهود والتدابير الحالية التي اتخذت حتى الآن للتعامل مع قضية الجريمة الإلكترونية مقيدة بالوقت والتواريخ، لأن الإنترنت في حالة تطوّر مستمر. لا يمكن لصنّاع القانون وإنفاذه في العراق مواكبة هذه التطورات السريعة. إن قطاع الإنترنت في العراق غير منظم حاليًا في هذه المرحلة الزمنية، ما يجعله من أكثر الفئات ضعفًا. يحث الوضعان السياسي والأمني الحالي في العراق على العمل الإضافي والضروري لتطوير الأسس القانونية والتقنية والتنظيمية وبناء القدرات لتوفير الأمن السيبراني الشامل لمواطنيها وأعمالها والحالة الهشة الحالية.

إن التعامل مع القضية العراقية ليس بسيطًا لأن البيانات الموثوقة حول أنواع الجرائم الإلكترونية في العراق غير كافية، ونادراً ما تنشرها الحكومة العراقية. ومع ذلك، تكشف التقارير الصادرة عن المنظمات غير الحكومية عن أكثر أنواع الجرائم الإلكترونية شيوعًا في العراق، والتي زادت بشكلٍ كبير خلال السنوات السبع الماضية.

تتم الغالبية العظمى من جرائم الإنترنت في العراق عبر منصات التواصل الاجتماعي، وعلى فيسبوك بشكلٍ أساسي، وضد الأشخاص بدلاً من الشركات أو الحكومات. تتضمن الهجمات الإلكترونية الأكثر شيوعًا الاحتيال عبر الإنترنت، سرقة الهوية، استغلال الأطفال في المواد الإباحية، مطاردة الإنترنت، الابتزاز الإلكتروني، انتهاك حقوق النشر، القرصنة عبر الأقمار الصناعية وإرهاب الإنترنت. لا يسع المرء إلا أن يعترف باحتياجات الفضاء السيبراني في المجتمعات كافة، ومع ذلك، يجب أن ندرك أن جرائم الإنترنت هي طفلها الوحش، وقد حيّرت باستمرارٍ المشرعين. إذا كان بناء قوانين مكافحة الجريمة الإلكترونية ممكن، فما مدى صعوبة المهمة؟ هل يؤدي ذلك إلى مشاكل أكثر من الحلول؟

تعد الاستجابة للجريمة السيبرانية في العراق بالتحديد أكثر صعوبة، لأن الاقتصاد في بلد مزعزع سياسيًا يفضل المجرمين. وباستخدام جهاز كمبيوتر محمول فقط، يمكن لفردٍ واحد أن يعيث فسادًا في الأفراد والمؤسسات بأقل تكلفة ممكنة وخطر التعرض للإصابة. الحل الوحيد الذي يمكن أن يقدّمه العراق هو التماس المزيد من التقنيات المتقدمة وإجراءات الحماية.