



IN PARTNERSHIP WITH
**FRIEDRICH NAUMANN
STIFTUNG** Für die Freiheit.
Middle East and North Africa



Cybercrime Laws in Arab Countries Focus on **Jordan, Egypt and the UAE**

Policy Paper, Prepared by Yahya Shqair

This study was developed under the supervision of Arab Reporters for Investigative Journalism (ARIJ) with the support of the Friedrich Naumann Foundation for Freedom

Table of Contents

Abstract

Introduction

CHAPTER 1: Characteristics of Digital Media

I: The status of digital media in the Arab region and its impact on traditional media

II: The direct impact of the spread of digital media on traditional Arab media

III: The increase in Internet access in Arab countries

CHAPTER 2: Cybercrime Laws in Arab Countries

Cybercrime Laws in Jordan, Egypt and the United Arab Emirates

Jordan

Examples of cybercrime penalties

Jordan

Egypt

The United Arab Emirates

An overview of legislation governing cybercrime in Arab countries

Palestine

Kuwait

Bahrain

Saudi Arabia

Sultanate of Oman

Qatar

Sudan

Syria

Algeria

Mauritania

Tunisia

Morocco

Iraq

Lebanon

Yemen

A comparison between the laws of cybercrime in the Arab countries



CHAPTER 3: International Standards for Freedom of Opinion and Expression on the Internet and their Legal Restrictions

Balancing the protection of privacy and national security, including the prohibition of discriminatory discourse and the protection of freedom of expression

Freedom of the press and media in the Arab countries

Conclusion

Recommendations

Appendix of the provisions of the laws of cybercrime in 13 Arab countries



Dear Reader,

It was the so-called “inventor of the internet”, Tim Berners-Lee, who proclaimed in the late 1990’s that the decentralized nature of the web gave him “tremendous hope” that we could “collectively make our world what we want.” For Liberals, the online revolution held a similarly amazing promise: the free flow of information, unhindered expression – regulated not by any central authority, but by individual responsibility and organic community norms.

The principal of “Freedom of Expression” has therefore become a central tenet of liberal thought, after a long struggle against state attempts to curb free thought and speech. And it is irrelevant if this liberty is under threat either offline or online. But what does that mean?

In theory – as is often the case – everything is rather clear. The expression of thoughts is an essential power for individuals. Albeit subject to restrictions when it poses a clear and direct harm to others – e.g. the famed shout of “fire” in the crowded theater – expression ought to remain as free as possible, whether online or offline. ‘Bad’ ideas are subject to being crowded out by better ones in a marketplace of ideas, rather than being shut down by a central power like a state. Innovative platforms will flourish, inefficient ones – those that do not provide for the free flow of information or constrain speech – will be marginalized as a result of informed consumer choices. The Arab uprisings seemed to leapfrog towards that ideal: All of a sudden, the state was not controlling public

opinion any longer; Facebook and other platforms had provided an innovative solution for the free exchange of ideas.

Yet the real world is – of course – more complex, and whenever false information is amplified, it poses an often indirect but real threat to the welfare of some. This threat is by no means trivial, but easily abused if framed as one against order and security. Whenever an idea is redefined as being “harmful”, the idea or the one who uttered it ought to be “cancelled,” or prevented from speaking in the first place. Authoritarian governments all over the world make use of this fact by now: If they decide what consists of hate-speech and what does not, dissent is easily criminalized. Regimes shut down social media to disrupt protests and governments institute internet blackouts.

Furthermore, whereas large online platforms may not limit individual speech as eagerly as some governments would like to, discussions over the extent to which algorithms – and those who design and own them – exert control over public opinion show a new set of questions that clash with liberal ideas about civic spaces.

I am saying all of this against the background of my experiences working for a “western” liberal Foundation in various parts of the MENA world over the past decade: After associating with

liberals in Egypt, Lebanon, Jordan and all over the Arab World, I have come to appreciate that we are all confronted with fundamentally different political, social, economic, religious and cultural challenges - and, therefore, are forced by circumstance to develop specific answers. Liberalism as such never offers a coherent set of answers to a wide range of problems. So what is liberalism's added value?

It is to fill, as pragmatically as possible, precisely this ill-defined space between the somewhat theoretical - the inherent value of free expression - and the very real: The threat of intrusive governments; the understandable urge to put a lid on ethnic hatred online, on the spread of terrorism or the encouragement of self-harm; the danger of foreign election interference; the unhealthy market effects of monopolies in network economies; the great potential of an online economy and the threats it poses to societal stability. In fact, this is where liberalism's core strength lies: to bridge the theoretical and the real, not just in abstract utopia, but pragmatically in all kinds of circumstances.

Even for dedicated pragmatists, however, a liberal perspective on how Arab governments have dealt with the internet and in particular issues of freedom online seems dismal: the simple truth is that in many places, a Facebook post can land even a tourist in prison. Nevertheless, liberals can offer solutions, tweaks, or incremental steps to greater freedom in all countries examined in this volume. Just as there is not one blueprint for liberal thought on free expression online, the region is quite diverse in its approaches,

ranging from severely clamping down on free expression to constitutionally safeguarding it.

Online pioneers' hopes, that we could "collectively make our world what we want", may not have come to full fruition, and less so where governments have historically been overbearing. Still, the internet and the ways citizens use it to freely express their thoughts, is not cast in concrete. Opportunities to shape it remain plentiful, since there is no world-wide standard of internet governance, nor a dominant approach stemming from either "the West," Europe, or China.

This publication will help engaged citizens, who care about freedom of expression online, take stock of how their region fares so far. Hence, the report is only a snapshot of current reality - however containing very valuable analysis, and equipped with a mandate to periodically reassess developments in the region. In doing so, it will remain relevant not only to a scholarly community, but to anyone impacted by developments in the field of internet governance and free expression: at a minimum this means all users of social media who are therefore being subject to often harsh cybercrime laws.

Dirk Kunze

Regional Director for Middle East and North Africa
Friedrich Naumann Foundation for Freedom

Abstract

The Internet is the most participatory form of mass communication in history and has evolved as a tool to seek, receive and impart information. Digital media has provided an unprecedented and historic opportunity for marginalised and voiceless communities to express their views and communicate with others. Internet penetration in the Middle East reached 67 percent in 2019 – higher than the global average.²

The ICT revolution has brought enormous benefits to humanity, but it has also provided new opportunities for illegal practices such as money-laundering, drug distribution and gambling, and a platform for crimes such as defamation, incitement to violence and hate speech. The misuse of this medium and its derivatives – such as social media platforms – is practiced by a minority and should not overshadow the Internet’s vast benefits.

Governments around the world have grappled with how to mediate this new media, often in terms of controlling its content. Arab governments in particular have confronted this new technology with a reactive rather than a proactive approach, often viewing the ICT revolution as a challenge to their authority rather than an opportunity. For example, 13 Arab countries have enacted legislation to deal with cybercrime, while the rest apply existing laws to these new crimes. Importantly, most cybercrime legislation in Arab states does not meet international standards of freedom of expression, instead surpassing legitimate restrictions in democratic systems by impeding dialogue and curbing freedom of expression.



Introduction

The Internet is the most efficient way to seek, receive and transmit information³. This contemporary medium of mass communication is a product of the integration of information and technology. Its development provides an unprecedented opportunity for citizens – especially those in marginalised communities or with limited freedom of expression – to communicate, access and share information. Internet penetration in the Middle East reached 67 percent in 2019, higher than the global average of 56.5 percent.⁴

This technology has provided tremendous benefits to people and society, but it has also created new avenues to commit crimes, such as distributing illegal drugs, inciting violence or sexually exploiting children. The technology itself, however, is inherently neutral: Its purpose is determined by its user, just as a kitchen knife can be a useful tool in a kitchen or a lethal weapon depending on the intent of the person using it. Similarly, social media platforms such as Facebook and Twitter connect people across the globe but can also be exploited to spread hatred and defame others. The potential for misuse should not overshadow the many benefits offered by the Internet.

This paper focuses on government efforts to combat cybercrimes and examines the impact of cybercrime legislation on freedom of expression in Arab

countries. It explores the compatibility of cybercrime laws with international laws and norms on freedom of expression and looks at how the right to freedom of expression is balanced with the protection of privacy and national security in Arab countries.

Globally, 138 countries have introduced cybercrime legislation.⁵ In the Middle East and North Africa (MENA), 13 Arab countries have passed specific legislation to combat cybercrime, while the rest have applied existing rules to these new crimes. This paper finds that cybercrime and media legislation in Arab countries impedes dialogue and curbs freedom of expression. Examples of restrictive provisions adopted in Arab laws include the following:

- In Egypt, every personal website, blog or social media account with more than 5,000 followers must be officially licensed in accordance with Law No. 180 of 2018 regulating the press and media.
- In the United Arab Emirates (UAE), the 2012 cybercrime law provides for the criminalisation of anyone who publishes information, news, statements or rumours on a website, computer network or information technology outlet with intent to make sarcastic remarks towards, or damage the reputation, prestige

³ "Reno v. American Civil Liberties Union, 521 U.S. 844 (1997)", Justia US Supreme Court, <https://supreme.justia.com/cases/federal/us/521/844/>

⁴ Anna Puri-Mirza, "Internet penetration rate in the Middle East and globally 2009 - 2019." Statista, May 28, 2019, <https://www.statista.com/statistics/265171/comparison-of-global-and-middle-eastern-internet-penetration-rate/>

⁵ "Cybercrime Legislation Worldwide," UN Conference on Trade and Development, https://unctad.org/en/Pages/DTL/STI_and ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx

or stature of, the State or any of its institutions, its president, vice-president, any of the rulers of the Emirates, their crown princes, the deputy rulers of the Emirates, or any national symbols such as the Emirati flag, emblem or anthem.

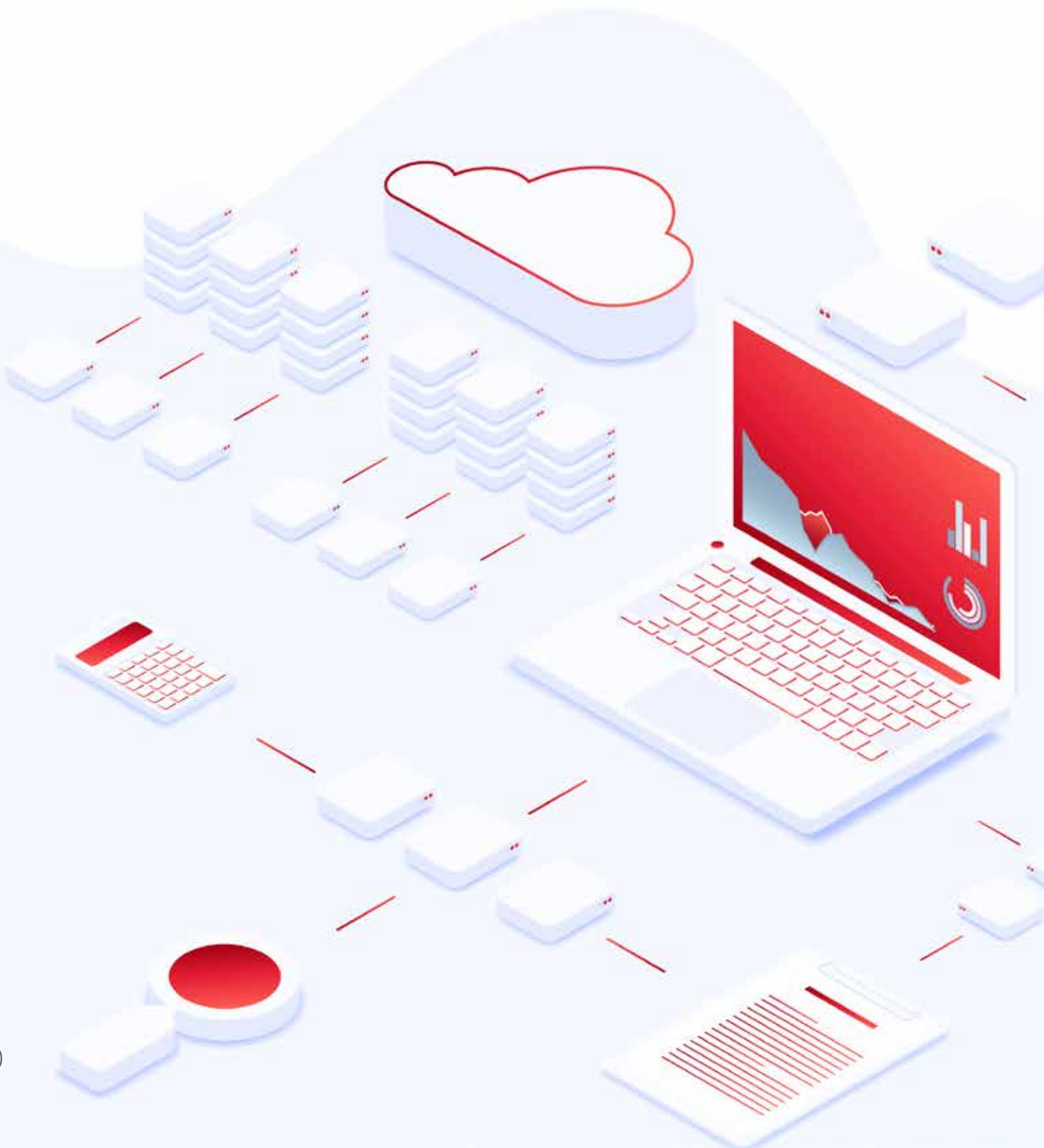
- In Saudi Arabia, the Press and Publications Law states: "If the infraction constitutes an offense against the Islamic religion or affects the higher interests of the country, it shall be submitted to the King for consideration of legal procedures to bring the case before the competent court, or to take such action as he deems in the public interest."

- In Sudan, the law provides for the punishment of flogging against anyone who uses any means of information, communication or applications to publish any news, rumour or report, knowing that it is untrue or published with the intention of provoking fear or panic among the public, threatening public safety, or undermining the prestige of the state.
- In Jordan, journalists and political activists can be remanded in custody under the cybercrime law in force.



CHAPTER 1

Characteristics of Digital Media





.1

The status of digital media in the Arab region and its impact on traditional media

Historically, ruling authorities have been quick to establish legal mechanisms to control new methods of mass communication. In Europe, the spread of the printing press, which began in the 15th century, was accompanied by efforts to censor and control it by state authorities and the Catholic church.⁶ Fear and distrust among ruling authorities and some clerics delayed the import of the printing press to the Arab world, and in 1941, Jordan banned ownership of homing pigeons.⁷ Arab governments today continue to see technological advances in mass communication as a challenge to their power rather than an opportunity, as reflected in modern-day restrictions on the Internet and social media platforms.⁸

Legislation in Arab countries is often developed by ruling elites and is not enacted in response to societal problems. The World Bank has described the MENA

region as “the least transparent in the world in terms of legislation and consultation with its people.”⁹ Besides the law, the media is also a critical tool of control.¹⁰ The press in Arab countries can be classified as “crowd-controlling and loyal [...] subject to the control of those who own it”.¹¹ Traditional Arab media lacks independence or freedom and instead is used as a tool to support governing authorities.

Researcher Walid Al-Saqaf has described control of information as a common feature of authoritarian regimes. “With the advent of the Internet, attempts to maintain a complete blackout of certain types of information, such as anti-regime messages and critical videos, have decreased,” according to Al-Saqaf.¹² “The majority of authoritarian regimes feel that the Internet is a threat to their rule, and therefore these regimes are trying to apply their past practices of censorship,” Al-Saqaf added.

⁶ Dr Jurgen Wilke, “Censorship and Freedom of the Press in Early Modern Europe,” Brewminate, February 12, 2018, <https://brewminate.com/censorship-and-freedom-of-the-press-in-the-early-modern-period/>

⁷ Article 2 of Pigeon Control Regulation No. 810 of 1941: “Non-official bodies are prohibited from acquiring a homing pigeon. Within 10 days of the publication of this law, those in possession of a messenger pigeon must hand it in to the authorities. Those in violation of the law shall be punished with the penalties stipulated in Article 4 of the Defense Law of 1935.”

⁸ Dr. Essam Al-Mousa (2014). “Digital Arab Media and Current Challenges,” Dar Ward - Safer Printing Press, Amman, Jordan.

⁹ The Bank has designed an index of 0 (the lowest score) to 5 (the highest score) to explore serious legislative practices in 186 countries. The Arab countries have ranked last, with Saudi Arabia, Libya, Yemen, Qatar and Syria scoring zero. Morocco scored 4, the highest Arab score, followed by the UAE (3.25) and Tunisia (2.5), Jordan and Bahrain (2). See: “Global Indicators of Regulatory Governance,” The World Bank, <https://rulemaking.worldbank.org/en/key-findings>

¹⁰ Herbert I. Schiller (1973). *The Mind Managers*. Boston: Beacon Press.

¹¹ William A. Rugh, “The Arab Press: News Media and Political Process in the Arab World,” Translation d. Musa al-Kilani, The Jordanian Books Centre, 1989, p.113.

¹² Article by researcher Walid Saqaf, who works at the University of Stockholm, Sweden

.2

The direct impact of the spread of digital media on traditional Arab media

The impact of digital media was demonstrated in its role in triggering the Tunisian revolution. On December 17, 2010, Tunisian street vendor Mohamed Bouazizi set himself on fire in front of Sidi Bouzid governorate headquarters after a police officer, Fadia Hamdi, confiscated goods from his vegetable cart. News of the incident spread on social media and ignited the revolution which would topple President Zine El Abidine Ben Ali. Hamdi had told Bouazizi “Dégage”, which means “Leave,” and this became a slogan of the Tunisian revolution and subsequent uprisings across the region. While the Bouazizi incident most notably led to the downfall of the Tunisian regime, the event also marked the beginning of a change in the Arab media system, in favour of new media and especially social media.¹³ The state, or those who controlled the press, no longer had a monopoly on broadcasting or publishing news, or in controlling public opinion.

New forms of media have also shifted the flow of information from vertical (those in power and news generators) to horizontal (citizen to citizen); the number of people engaged in communication and networking has increased with the expansion of freedom of expression, all of which has made it difficult for governments to control the media as

they had in the past. New media has also expanded citizens’ perceptions of their rights and freedoms; when rights have been transgressed, it has offered a way to appeal to public opinion that is perhaps faster than appealing to the judiciary. New media has also been used to pressure decision makers in executive or legislative branches. Meanwhile, access to the new media market is easier and less expensive than the print media, which requires capital, office space, employees, ink and printing presses, and which has a shrinking readership. Globally, the distribution of print publications is in decline and advertisement revenue has migrated online.

In Lebanon, many prestigious print publications have closed, such as As-Safir in 2016, Al Ittihad in 2017, and Al Mustaqbal, which stopped printing in February 2019, as well as all Dar Al Sayyad publications. In Jordan, the daily Al Arab Al Youm closed in 2013, and Ad Dustour (the oldest Jordanian newspaper) suffered losses that exceeded its capital, while Al Rai’s share price fell to less than half a dollar.¹⁴ Its share price had been higher than that of the largest Jordanian bank and before 2010, its daily ad revenues were equivalent to five kilograms of gold.

¹³ Matt J. Duffy, “Arab Media Regulations: Identifying Restraints on Freedom of the Press in the Laws of Six Arabian Peninsula Countries,” Berkeley J. Middle E. & Islamic L. 1 (2014) <<https://heinonline.org/HOL/LandingPage?handle=hein.journals/bjme6&div=3&id=&page>> Also: Soengas-Pérez, Xosé (2013). The Role of the Internet and Social Networks in the Arab Uprisings an Alternative to Official Press Censorship. *Comunicar*, 2013, vol. 21, n. 41, pp. 147-155. <<http://eprints.rclis.org/19787/1/en147-155.pdf>> Also: Yahia Shukkeir, “New media in social resistance and public demonstrations,” Global Information Society Watch, 2011, <<https://www.giswatch.org/en/country-report/freedom-expression/jordan>>

¹⁴ Amman Stock Exchange Bulletin, May 5, 2019.

.3

The increase in Internet access in Arab countries

The gap in trust between the Arab public and the Arab media stems from the media's failure to meet the public's demand for information. Instead, this demand has been met by social media platforms.

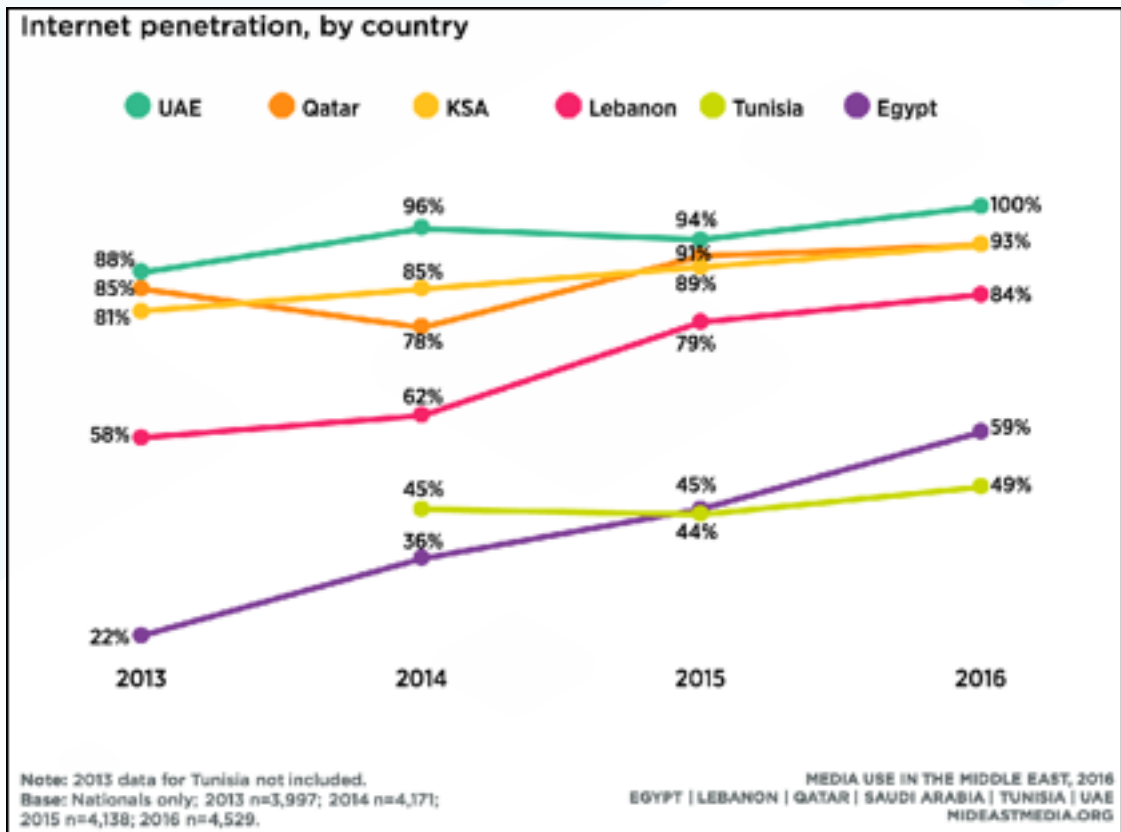
The infographic below shows the number of digital media users in the world per minute.¹⁵



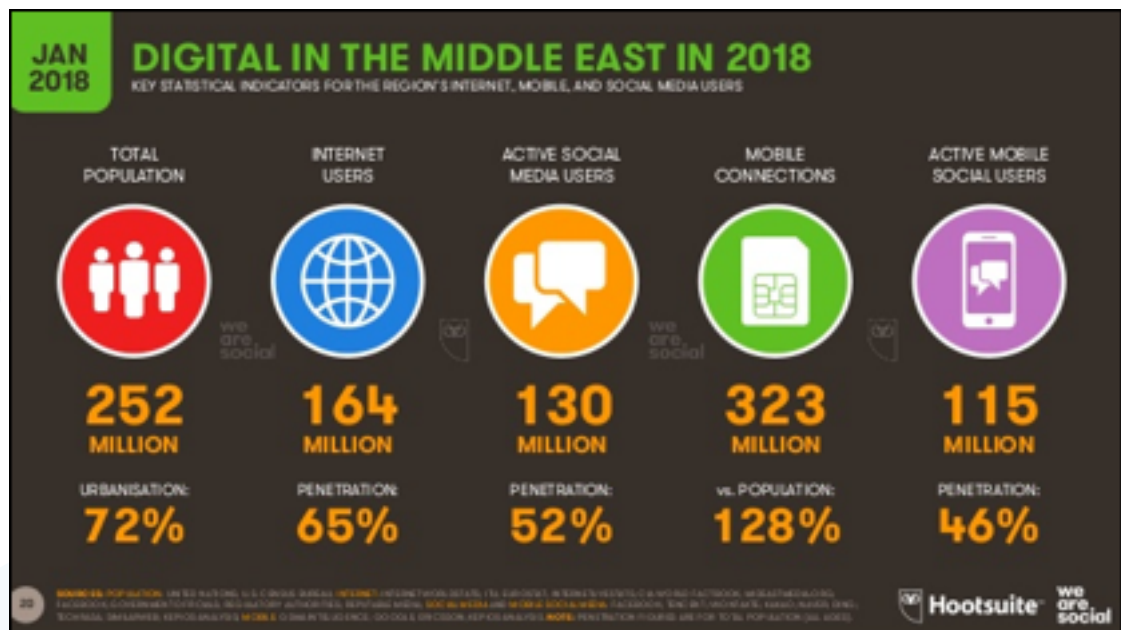
A study by Northwestern University in Qatar¹⁶ found that half of Arab citizens use the Internet, while more than two-thirds rely on their smartphones to follow the news.

¹⁵ "What happens in an internet minute," Visual Capitalist, March 13, 2019, <https://www.visualcapitalist.com/what-happens-in-an-internet-minute-in-2019/>

¹⁶ "Smartphones and the internet cited as primary sources of news consumption in Arab world," Northwestern University, November 1, 2017, <https://phys.org/news/2017-11-smartphones-internet-cited-primary-sources.html#jCp>



Rates of Internet access in select Arab countries in 2016. ¹⁷



The use of digital media in the Middle East. ¹⁸

The use of digital media in Arab countries is expected to grow alongside the emergence of a new spectrum of media platforms and the growing phenomenon of the “digitisation of media.” This coincides with the increased use of broadband Internet in the Arab region and the rise in media content views on mobile phones. ¹⁹

¹⁷ “Media Use in the Middle East, 2016” Northwest University in Qatar, <http://www.mideastmedia.org/survey/2016/chapter/online-and-social-media/>

¹⁸ “Digital in 2018 Global Overview,” January 29, 2018, <https://www.slideshare.net/wearesocial/digital-in-2018-global-overview-86860338>

¹⁹ Dubai Press Club (2016), “Arab media outlook: Youth... Content... Digital Media,” <http://www.dmi.gov.ae/program-detail.asp?PID=35304&PTID=41&lang=en#>

CHAPTER 2

Cybercrime Laws in Arab Countries



Globally, there have been three broad approaches to combating electronic crimes:

1. Regulation through public criminal law, particularly in the Penal Code (such as in Iraq) or through amended or complementary penal laws (such as in Morocco).
2. Incorporation of new legislation into the existing laws of publications or media (such as in Saudi Arabia).
3. Adoption of separate cybercrime laws, as in most Arab countries.

Thirteen Arab countries have enacted separate cybercrime laws. The first was the UAE, which enacted the IT Crimes Act (Federal Law No. 2 of 2006, amended three times in 2012, 2016 and 2018). Saudi Arabia enacted the Information Technology Crimes Act in 2007 (1428H), Sudan issued a law to combat these crimes in 2007 (amended in 2018), followed by Algeria in 2009 and Jordan in 2010 (a temporary law that was made permanent in 2015). Oman enacted legislation to combat IT crimes in 2011 after incorporating some provisions to combat these crimes into the Penal Code. Syria passed a law on electronic crimes in 2012, followed by Bahrain and Qatar in 2014, then Kuwait in 2015, Mauritania in 2016 and finally Egypt and Palestine in 2018.



Cybercrime Laws in Jordan, Egypt and the United Arab Emirates

Jordan

Jordan's connection to the Internet began in April 1996. The following year, the first Internet café was established and shortly after, Shafiq Irshaidat Street in Irbid, northern Jordan, set a world record for the highest number of Internet cafés on one street, occupying a position in the Guinness Book of Records. At the time, the Jordanian government's attempts to regulate the functioning of Internet cafés aimed to prevent adolescents from using them. In late 2000, the government issued instructions through the Official Gazette prohibiting those under the age of 16 from entering these cafés. It also stipulated that the cafés should be at least 500 metres away from the nearest mosque or church (notably, this provision also applies to liquor stores), and required café owners to

keep records of customers' names and the times of their visits. Following a debate about the illegality of such procedures, they were cancelled by the Minister of Interior within three weeks.²⁰

The Telecommunications Act (No. 13 of 1995, as amended by Act No. 21 of 2011) provided in article 75a: "Any person who, by any means of communication, sends threatening, insulting or immoral messages or transmits fabricated news with a view to provoking panic shall be punished with imprisonment for a minimum period of one month and a maximum period of a year, or a minimum fine of 300 Jordanian dinars (JOD) and a maximum fine of 2,000JOD, or both of these penalties."

The development of legislation governing cybercrime in Jordan

Jordan passed the Temporary Information Systems Crimes Act²¹ No. 30 of 2010, which was transformed into a permanent law under the name of the Cybercrime Law²² No. 27 of 2015. This law criminalises illegal access to the information network, changing or deleting the contents of a website, publishing or sending pornographic acts relating to the sexual exploitation of children, or promoting prostitution.

Article 11 of the Cybercrime Law is one of the most controversial parts of this law, due to its impact on freedom of expression and

opinion. Article 11 imposes a minimum prison sentence of three months and a fine of between 100 JOD and 2,000 JOD on anyone who intentionally transmits or publishes data or information that is defamatory or causes contempt for any person through an information network, website, or any information system. This allows for the imprisonment of journalists for publishing reports, overturning protections for journalists in the Press and Publications Act of 1998 and the Audiovisual Act of 2015 which did not provide for the arrest of journalists,

²⁰ Al Arab Al Youm newspaper published a study by journalist Yehia Shqair on the illegality of these instructions on January 8, 2001, which led the Minister of Interior to cancel them. See: "Media in the Arab States," Arab Centre for the Rule of Law and Integrity and the United Nations Development Program, 2007 Beirut, p.141. www.arabruleoflaw.org/Files/

²¹ The law was published in the Official Gazette number 5056 dated September 9, 2010, p.5334.

²² The original text of the law was published on page 5631 of the Official Gazette no. 5343 dated June 1, 2015. <<http://moict.gov.jo/uploads/Policies-and-Strategies-Directorate/Legislation/Laws/Electronic-crime-Law.pdf>>

instead imposing fines and compensation to the victim. The Publications Law regulates Jordanian daily newspapers (10), weekly newspapers (17), licensed websites (182) and other publications. The Audiovisual Act applies to 36 satellite stations and 38 broadcasters.²³ The Jordan Press Association, along with many local and international civil society organisations concerned with freedom of expression, raised objections to the Cybercrime Law.

In 2017, the government proposed changes to the Cybercrimes Law and in September 2018, the parliament referred the amendments to the parliamentary legal committee for discussion. In the amendments, the government proposed a broad definition of hate speech as any statement or act “intended to incite sectarian or racial strife or advocate violence, or to incite conflict between communities and various elements of the nation.” The definition proposed by the government was a word-for-word copy of article 150 of the Penal Code²⁴ with the addition of the clause on advocating violence. Under Article 10a of the amended draft law, whoever publishes “hate speech” through any network, website or information system shall be punished by imprisonment for at least three months²⁵ and fined between 5,000 and 10,000 JOD. The government also added Article 13, which imposes imprisonment of between three months and two years and a fine of between 1,000 and 2,000 JOD on

anyone who publishes or broadcasts rumours or news with the knowledge of its false nature, with intent or in bad faith.

The proposed amendments were rejected by multiple unions, parties and international organisations such as Amnesty International²⁶ and Human Rights Watch.²⁷ The amendments were also criticized at Jordan’s Universal Periodic Review at the United Nations Human Rights Council in Geneva in November 2018. The Jordanian government eventually withdrew the amended bill in December 2018 but announced a second draft law within 48 hours, without consultation with stakeholders such as MPs, journalists and civil society.

The House of Representatives rejected the new draft law on February 19, 2019.²⁸ Under the constitution, the draft law was then sent to the Senate for discussion. At the close of 2019, it appeared that the draft law would be rejected, and the original law No. 27 of 2015 would remain in force.

In this context, Dr Nahla Al-Momani, Head of Legislation Department at the National Centre for Human Rights,²⁹ has said that “Jordanian legislation did not balance between private life and freedom of expression. It did not clarify whether criticism of public figures on the basis of permissible criticism was not in breach of freedom of expression”.

²³ Media Commission website (statistics accessed on April 27, 2019) as of 27/4/2019) <<http://www.mc.gov.jo/Pages/viewpage?pageID=34>>

²⁴ Article 150 of Penal Code: Any writing and any speech or action intended or resulting in inciting sectarian or racial strife or inciting conflict between sects and the various elements of the nation shall be punished by imprisonment for six months to three years and a fine not exceeding two hundred dinars.

²⁵ According to Article 26 of the Penal Code, the maximum period of imprisonment is three years, which means that anyone who publishes hate speech may be arrested. If the minimum period of imprisonment is specified and the maximum is not specified, the maximum shall be three years.

²⁶ “Jordan: Government should withdraw amendments to cybercrimes law ahead of UN review,” Amnesty International, November 7, 2018, <https://www.amnesty.org/en/latest/news/2018/11/jordan-government-should-withdraw-amendments-to-cybercrimes-law-ahead-of-un-review/>

²⁷ “Jordan: ‘Fake News’ Amendments Need Revision,” Human Rights Watch, February 21, 2019, <https://www.hrw.org/news/2019/02/21/jordan-fake-news-amendments-need-revision>

²⁸ <https://alghad.com/%d9%82%d8%a7%d9%86%d9%88%d9%86-%d8%a7%d9%84%d8%ac%d8%b1%d8%a7%d8%a6%d9%85-%d8%a7%d9%84%d8%a5%d9%84%d9%83%d8%aa%d8%b1%d9%88%d9%86%d9%8a%d8%a9-%d9%88%d8%ad%d8%b1%d9%8a%d8%a9-%d8%a7%d9%84%d8%aa%d8%b9/>

²⁹ Correspondence with the author of the paper on April 7, 2019.

Examples of cybercrime penalties

Jordan

Another concerning aspect of the Cybercrime Law is that it allows suspected violators to be tried at the State Security Court. Senior Muslim Brotherhood official Zaki Bani Rshaid was tried before the State Security Court for “disturbing Jordan’s relations with a foreign state” over a Facebook post he wrote in November 2014 in which he accused UAE authorities of sponsoring terrorism and acting as a “policeman” for the United States. He was sentenced to 18 months in prison in February 2015.³⁰ In 2002, opposition activist Tujan Faisal, the first female deputy to be elected to the House of Representatives, was tried by the State Security Court for publishing an online letter criticising a former prime minister. She was convicted under a law promulgated by a provisional royal decree two weeks after the September 11 attacks in 2001 that expanded the definition of “terrorism.” Faisal was sentenced to eighteen months’ imprisonment, in a move viewed as an attempt to prevent her participating in parliamentary elections.³¹

Egypt

Egyptian authorities have a record of restricting freedom of opinion and expression and the media. Egypt ranked 163rd out of 180 countries in the 2019 Press Freedom Index compiled annually by Reporters Without Borders.³²

Law No. 175/2018 on combating information technology crimes³³ establishes the collective control of telecommunications in Egypt. Internet Service Providers (ISPs) are required to retain and store customer usage data for 180 days, including data that allows user identification, and data related to information system content or equipment used. This means that ISPs can obtain data on all user activities, including phone calls, text messages, websites accessed and applications used. The law grants national security agencies (Presidency, Armed Forces, Ministry of Interior, General Intelligence,

and Administrative Control Authority) the right to access the data held by ISPs, which are obliged to provide “technical capabilities” to these entities.

The law also allows investigators to block websites or content criminalized by the anti-cybercrime law, that constitutes a threat to national security or endangers the Egyptian economy. Individuals suspected of violating the law can be placed on a watch list and prevented from leaving the country. Content that violates the principles or family values of Egyptian society or the sanctity of private life is criminalised and punishable by up to six months in prison and a fine of between 50,000 and 100,000 Egyptian pounds. This law has been criticised for its broad and ambiguous terms. For example, the phrase “family principles or values in Egyptian society, harm to national unity and social peace” does

³⁰ “Jordan: 18 Months for Criticizing UAE,” Human Rights Watch, February 19, 2015, <https://www.hrw.org/news/2015/02/19/jordan-18-months-criticizing-uae>

³¹ “The Jordanian State Security Court sentenced Tujan Faisal to one and a half years in prison and a fine of 20 dinars,” Al Sharq Al Awsat, May 17, 2002, <https://archive.aawsat.com/details.asp?issueno=8435&article=103712#.XS1ibGS8bcs>

³² “2019 World Press Freedom Index,” Reporters Without Borders, <https://rsf.org/en/ranking>

³³ Published in the Official Gazette, August 14, 2018


not clearly define what is permitted and what is prohibited. International organisations have criticised the law's incompatibility with international standards for freedom of expression.³⁴

Article 19 of Law No. 180/2018 on the organisation of the press and the media³⁵ prohibits newspapers, media outlets and websites from publishing or broadcasting false news; advocating or inciting violence, hatred or a violation of the law; or discriminating between citizens. It also prohibits calls for racism or intolerance; insults or defamation of individuals; and insults aimed at religion or religious beliefs. This law applies to every personal website, personal blog or personal social media account with 5,000 or more followers.³⁶

An unusual provision that is unique to Arab legislation

Law No. 2018/180 on the organisation of the press and media in Egypt is applied to every personal website, blog or personal social media account with 5,000 or more followers.

Under Article 19, Egyptian authorities blocked 34,000 websites in an effort to undermine a campaign opposing an amendment to the Egyptian constitution³⁷ in April 2019, according to NetBlocks, which advocates for an open and inclusive digital future.



| cca2 | country | site | state | failure_rate | reachability | failrate | rtt |
|------|---------|-------------------------|-------|--------------|--------------|----------|-----|
| SD | Sudan | https://voiceonline.net | DOWN | | 0% | 100% | 2 s |
| EG | Egypt | https://voiceonline.net | DOWN | | 25% | 75% | 2 s |

This image shows the blocking of the #Voiceonline campaign opposing the amendment of the Egyptian constitution.

It is clear that many provisions of Egyptian laws do not conform to international standards, including in their broad definitions and disproportionate penalties. However, the Egyptian judiciary has a legacy of balancing freedom of opinion and expression with its limitations. For example, the Supreme Constitutional Court in Egypt decided: "It is dangerous to impose restrictions that strain the freedom of expression to repel citizens from exercising it."³⁸ The Constitution provides for freedom of discussion and dialogue in all matters relating to public affairs, even if it is critical of officials.

³⁴ "Statement opposing Egypt's legalisation of website blocking and communications surveillance," Euromed Rights, September 7, 2018, <https://euromedrights.org/publication/statement-opposing-egypts-legalization-of-website-blocking-and-communications-surveillance/>

³⁵ Published in the Official Gazette on August 27, 2018. <<http://www.rosaelyoussef.com/news/details/374017>>

³⁶ A similar text exists in China and Russia. See: "Freedom on the Net 2018: The rise of Digital Authoritarianism," October 2018, Freedom House, https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf

³⁷ "Egypt filters 34,000 domains in a bid to block opposition campaign platform," Netblocks, April 15, 2019, <https://netblocks.org/reports/egypt-filters-34000-domains-in-bid-to-block-opposition-campaign-platform-7eA1b1Bp>

³⁸ Dr. Ali Awad Hassan, Case No. 42 of 1995 in Legislative Texts Ruled Unconstitutional, (Alexandria: Alexandria University Press, 1996).

The United Arab Emirates

In 2006, the UAE became one of the first countries to pass a Cybercrime Act. This was amended by Federal Law No. 5 of 2012 on combating cybercrimes³⁹ and again in 2016 and 2018.

Under Article 20 of Federal Law No. 5 of 2012, insulting or slandering another person online or through any use of information technology is punishable by imprisonment and/or a fine of between 250,000 and 500,000 dirhams. Slander or insult of a public official or public servant is considered an aggravating circumstance.

Article 24 states that anyone who creates or runs a website or publishes information on a computer network or an information technology medium to promote any programmes or ideas that may provoke sedition or hatred, racism or sectarianism, damage to national unity or social peace, or disruption of public order or morals shall be punished with

temporary imprisonment and a fine of between 500,000 and 1 million dirhams.

According to Article 26, whoever creates or runs a website or publishes information on the Internet or other information technology mediums for a terrorist or illegal group, association or organisation, with the intent of facilitating contact with its leaders or members, attracting members, promoting its ideas, financing its activities, providing assistance, or promoting the manufacture of incendiary devices or explosives or any other tools used in terrorist acts, shall be punished by imprisonment for between 10 and 25 years, and fined between 2 million and 4 million dirhams.

The Court may order the surveillance of an individual convicted of an offense under the anti-cybercrime law, or prohibit the individual from using any computer network or information technology for a period of time.

³⁹ Published on August 13, 2012 Available at: <https://elaws.moj.gov.ae/UAE-MOJ_LC-Ar/00_%D8%AC%D8%B1%D8%A7%D8%A6%D9%85%20%D8%AA%D9%82%D9%86%D9%8A%D8%A9%20%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA/UAE-LC-Ar_2012-08-13_00005_Markait.html?val=AL1#Anchor11>

UAE law is the most stringent among Arab states. It includes punishments that limit freedom of expression and imposes disproportionate penalties for online publishing. UAE law is unique in criminalising acts that are not mentioned in any other Arab laws.

Article 27 prohibits the use of computer networks or information technology to promote or collect donations without a license.

Article 29 prohibits the publication of information, news, statements or rumours on a website, computer network or information technology medium with intent to practice sarcasm or damage the reputation, prestige or stature of the State or any of its institutions or its president, vice-president, any of the rulers of the Emirates, their crown princes, or the deputy rulers of the Emirates, the State flag, the national peace, the Emirati emblem, anthem or any of its symbols.

Article 32 prohibits establishing or running a website or using a computer network or any information technology medium to plan, organise, promote or call for demonstrations or protests or the like without a license.

Article 38 criminalises anyone who provides any organisations, institutions, authorities or any other entities through the computer network or any information technology medium with incorrect, inaccurate or misleading information which may damage the interests of the State or injure its reputation, prestige or stature.

The use of broad, imprecise language such as “publishing or broadcasting information, news, cartoons, or any other images that endanger the security and supreme interests of the state, or prejudice public order” is incompatible with international standards which require that the law must be clear. These broad terms may allow law enforcement officials to further criminalise acts that the legislator may not have intended to criminalise.

The UAE has not ratified the International Covenant on Civil and Political Rights, Article 19 of which gives the right to freedom of opinion and expression. However, it is a member state of the Arab Charter on Human Rights, and Article 32 of the Charter guarantees freedom of information and freedom of opinion and expression. Article 24 of the Charter also includes the right to freedom of political activity, the right to join and form associations, and the right to freedom of assembly.

International organisations have repeatedly criticised the UAE's anti-cybercrime law, including Human Rights Watch which has described it as a tool to close the only remaining forum for free expression in the country. Self-censorship is widespread in the UAE due to the strict laws and excessive penalties.⁴⁰

As an example of disproportionate sentences, a citizen was sentenced to 10 years' imprisonment in March 2019 after being convicted of creating several social media accounts (on Facebook and Twitter). He was also convicted of publishing "false and malicious information that are unfounded, offend the UAE society, incite sectarian strife, and harm social cohesion and national unity" in violation of Federal Law No. 5 of 2012 on combating cybercrime.⁴¹

In 2015, the UAE sentenced Jordanian journalist Tayseer Al-Najjar to three years in prison and a fine of 500,000

dirhams (USD 135,000) for a Facebook post criticising the UAE's stance on the 2014 Israeli war on Gaza. The court found this was an insult to state symbols and violated Article 29 of Federal Law Decree No. 5 of 2012 on combating cybercrime. Al-Najjar remained in prison after serving his sentence at the end of 2018 because he had not paid the fine. Under UAE law, a person can be imprisoned for an extra day for every 100 dirhams of an unpaid fine up to a maximum of six months.⁴² Al-Najjar was eventually released on February 12, 2019, without paying the fine, and he returned to Jordan.

In a case that has drawn the attention of the United Nations High Commissioner for Human Rights, Michelle Bachelet, prominent Emirate human rights defender Ahmed Mansour was convicted in May 2018 of using social media to "spread false information that harms national unity and the country's reputation" in tweets critical of the government. The UAE State Security Court sentenced Mansour to 10 years' imprisonment and a fine of 1 million dirhams (USD 272,000). On January 4, 2019, Bachelet expressed concern that Mansour was being punished for exercising the right to freedom of expression and opinion. She called for Mansour's immediate and unconditional release and urged the UAE government to ensure individuals were not punished for expressing views critical of the government or its allies.⁴³

⁴⁰ "UAE: Cybercrimes Decree Attacks Free Speech," Human Rights Watch, November 28, 2012, <https://www.hrw.org/news/2012/11/28/uae-cybercrimes-decree-attacks-free-speech>

⁴¹ "10 years imprisonment for a social media user that offended the Emirates," Emarat Al Youm, March 27, 2019. <https://www.emaratalyoum.com/local-section/accidents/2019-03-27-1.1196631>

⁴² "Government official: Journalist Al-Najjar is required to pay a fine or remain in prison for 6 months," Al Mamlaka TV, December 25, 2018, <https://www.almamlakatv.com/news/-11325البقاء-أو-غرامة-بدفع-ملزم-النجار-الصحفي-النجار-ملزم-بدفع-غرامة-أو-البقاء-11325>

⁴³ "Briefing note on the United Arab Emirates," Office of the UN High Commissioner for Human Rights, January 4, 2019, <https://www.ohchr.org/AR/NewsEvents/Pages/DisplayNews.aspx?NewsID=24054&LangID=A>

.2

An overview of legislation governing cybercrime in Arab countries

Palestine

The first decision issued by the late Palestinian President Yasser Arafat after the establishment of the Palestinian National Authority was Resolution No. 1 of 1994, published in the Official Gazette (Palestinian Chronicle), which revived laws and legislation that were in force before the Palestinian territories fell under Israeli occupation in 1967.

The Chairman of the Executive Committee of the Palestine Liberation Organisation, the President of the Palestinian National Authority, based on the decision of the Executive Committee, and on the authority vested in him, decided the following:

Article 1: The laws, regulations and orders that were in force before June 5, 1967 shall continue in the Palestinian territories (West Bank and Gaza Strip) until they are consolidated.

This reinstated the Jordanian Penal Code as the legal code of the Palestinian National Authority, as it stood before the June 1967 war and without amendments made in Jordan since 1967. In Gaza, the Palestinian Penal Code (the British Mandate Act of 1936) is applied, which is more protective of public freedoms than its Jordanian counterpart. This is just one example of the chaos of legal norms in Palestine, the dualism of the West

Bank and Gaza, and the division between Fatah, which governs the West Bank, and Hamas, which rules the Gaza Strip.

One of the early laws promulgated by Arafat was the Palestinian Publications Law of 1995, a replica of the Yemeni Publications Law (and not the Jordanian, as it is mistakenly believed). Although Yemeni law does not impose penalties of detention, Palestinian law has added to it the penalty of imprisonment.

The issuance of the decree on the cybercrime law No. 16 of 2017 in Palestine was criticised by Palestinian civil society organisations and human rights groups. In response to these criticisms and pressures, Law No. (10) of 2018 on cybercrime was issued.⁴⁴ Palestinian law, unlike other Arab laws, is notable for recalling the freedom of expression and opinion of every human being, as well as the freedom of the print and broadcast media.

The law criminalises anyone who uses electronic networks or information technology devices to threaten or blackmail another person, in particular threatens to commit a felony, an offense which is punishable by imprisonment (Article 15). It also punishes the sending of pornography, especially to children. Arbitrary or unlawful interference with the privacy of any person, family, home

⁴⁴ Decree Law No. 10 of 2018 was published in issue no. 16 of "Palestinian Facts" issued June 20, 2018, p.8.

or correspondence is prohibited. The law also criminalises racial or religious hatred or racial discrimination against a particular group because of their ethnic or religious affiliation, colour or disability.

The Independent Palestinian Commission for Human Rights welcomed the issuance of Law No. (10) of 2018 on Cybercrime.⁴⁵ The Commission highlighted in a statement that its main objections to the former cybercrime law No. 16 of 2017 related to its general provisions, as well as its excessive sanctions. Problematic aspects in the 2017 law included provisions that constituted a real and serious threat to the rights to freedom of opinion and expression and the right to privacy. The Commission also monitored several violations in the 2017 law, such as the arrest, summons and prosecution of journalists, activists and citizens for expressing opinions or for working in journalism.

Nibal Thawabteh⁴⁶, director of the Media Development Centre at Birzeit University in Palestine, expressed her support for the

demands of the Independent Commission for Human Rights. She noted that the unity of the parties in demanding the amendment of the law and the limited government response to these demands was a success that should be built on to secure further amendments to provisions that were outdated in the era of openness. She called for intensifying efforts to exert pressure on the government “to adopt the drafts of the rest of the laws governing the media such as the Supreme Council of Information, the Journalists’ Syndicate, the Audio-visual Commission, and the right to information, as well as the amendment of the law of publications and publishing, especially as the law of cybercrime is based on old laws to criminalise some practices.”

Palestinian citizens are subjected to censorship from three authorities when using social media:⁴⁷ the Fatah-led Palestinian Authority in the West Bank, which targets its opponents in Hamas; the Hamas-run de facto authority in Gaza, which targets its Fatah opponents; and the occupation authorities, which periodically detain Palestinians on the pretext of spreading what they claim to be “incitement to violence.”⁴⁸

⁴⁵ “The Commission welcomes the issuance of Resolution no. 10 of 2018 regarding cybercrime and provides observations and reservations,” Independent Commission for Human Rights, May 5, 2018, <https://ichr.ps/ar/1/26/2389/>-بشأن-(10)-لسنة-2018-الهيئة-ترحب-بصدور-القرار-بقانون-رقم-(10)-لسنة-2018-الجرائم-الإلكترونية-وتقدم-مجموعة-من-الملاحظات-والتحفظات.htm

⁴⁶ Correspondence with the author on May 9, 2019.

⁴⁷ “Internet Freedoms in Palestine: Mapping of Digital Rights Violations and Threats (2018),” Zameleh Arab Centre for Social Media Advancement, p.34. <http://7ameleh.org/wp-content/uploads/2018/01/7ameleh_Internet_Freedoms_in_Palestine.pdf>

⁴⁸ “Two authorities, one way, opposition is forbidden. Arbitrary Detention and Torture under the Palestinian Authority and Hamas,” Human Rights Watch, October 23, 2018, <https://www.hrw.org/ar/report/2018/10/23/323462>

Kuwait

Kuwait has three main laws on cybercrimes: Law No. 8 of 2016 on the Regulation of Electronic Media; the Cybercrime Law; and the Communications Law.

Law No. 8 of 2016 on the Regulation Of Electronic Media prohibits websites and electronic media subject to its provisions from publishing, broadcasting or transmitting content that violates the prohibitions set out in Articles 19, 20 and 21 of the Press and Publications Law. These articles restrict content relating to the Islamic religion or the Emir, and prohibit contempt of the constitution, indecent assault, the publication of confidential documents, and content that prejudices the privacy of persons or damages relations with Arab and friendly countries. The law permits a temporary blocking of websites or media under investigation or on trial.

The Cyber Crime Law⁴⁹ No. 63 of 2015 criminalises the threat or extortion of a

person with a minimum penalty of five years in prison and a fine of between 5,000 and 20,000 Kuwaiti dinars (Article 3). Article 10 states that creating a website for a terrorist or a terrorist organisation, or using the Internet or information technology to promote terrorist ideology, finance terrorism, facilitate contact with members of terrorist organisation or disseminate information on how to make incendiary or explosive devices or instruments used in terrorist acts is punishable by up to 10 years' imprisonment and a fine of between 20,000 and 50,000 Kuwaiti dinars.

Under Law No. 37 of 2014, which established the Communications and Information Technology Regulatory Authority, using telecommunications devices to send threats or "immoral messages," or to transmit fabricated news to create panic is punishable by up to two years' imprisonment and a fine of up to 5,000 Kuwaiti dinars.

⁴⁹ The law came into force on January 12, 2016, six months after its publication in the Official Gazette on July 7, 2015.

Law No. 60 of 2014 on cybercrime⁵⁰ and its amendments criminalise the use of the Internet to disseminate pornographic content, with higher penalties imposed if the offense involves children.⁵¹ Article 23 states that acts criminalised in other laws shall receive the same penalty if they are committed using information technology, with the exception of offenses described within Law No. 60/2014.

Bahrain's Penal Code, enacted by Law No. 15 of 1976, criminalises the broadcast of false or malicious news, statements or rumours about the domestic situation of the state, or that undermines financial confidence in the state or negatively affects its prestige, as well as activities that harm national interests (Article 134).⁵² The broad and vague language in the text of this article means it fails to define clearly what is permissible or prohibited.

Article 165 of the Penal Code is also controversial, mandating the imprisonment of anyone who incites hatred or hostility toward the regime. The Bahrain Independent Commission of Inquiry⁵³ has expressed concern

that this article has been applied "in a manner that infringes upon the freedoms of opinion and expression." The commission stated in a report that opinions expressing opposition to the existing regime in Bahrain or calling for any peaceful change in the structure or system of government or for regime change have been excluded from public debate by Article 165.⁵⁴ The Committee complained that articles 165, 168 and 169 of the Penal Code restricted freedom of expression by criminalising incitement to hatred of the regime or harming the public interest without requiring any material act that causes social or individual harm. "[These articles] have been applied to repress legitimate criticism of the government of Bahrain," the Commission wrote.⁵⁵

The spirit of article 165, and the criminalisation of dissent, has a long history. In Egypt, a decree was issued in March 1929 imposing imprisonment and/or a fine on anyone who incited hatred or contempt for the regime. This remains in force in Article 174 of the Egyptian Penal Code. Similarly, in the United States the Contempt Act of 1789 imposed fines of USD 5,000 and five years' imprisonment

⁵⁰ "Cybercrime Law in the Kingdom of Bahrain - Law no. 60 of 2014," General Directorate of Anti-Corruption & Economic & Electronic Security - Cyber Crime Directorate. September 30, 2014, <http://www.acees.gov.bh/cyber-crime/anti-cyber-crime-law-in-the-kingdom-of-bahrain/>

⁵¹ Bahrain has acceded to the two Optional Protocols on the involvement of children in armed conflict and the sale of children, child prostitution and child pornography in the United Nations Convention on the Rights of the Child by Law No. 19 of 2004.

⁵² Amended by Law No. 51 of 2012 Amending Certain Provisions of the Penal Code Published in the Official Gazette on October 11, 2012 No. 3073).

⁵³ The Bahrain Independent Commission of Inquiry (BICI) was established under the chairmanship of the Egyptian expert in international law d. Mahmoud Sharif Bassiouni on June 29, 2011 under Royal Order No. 28 of King Hamad bin Isa Al-Khalifa. The Commission was entrusted with the task of investigating the events that took place in Bahrain that year and the consequences of those events.

⁵⁴ "Report of the Bahrain Independent Commission of Inquiry," Bahrain Independent Commission of Inquiry, <http://www.bici.org.bh/BIClreportEN.pdf>, Paragraph 1281 p.311.

⁵⁵ Ibid. Paragraph 1284, p.312.

for anyone convicted of writing, printing or publishing anything false against the US government, Congress, its members or the president with the intent to expose any of them to contempt. The law lasted for several months, until President Thomas Jefferson pardoned all those found guilty of violating the law and returned the fines they paid.

Article 172 of Bahrain's Penal Code states that using any method of publication to incite hate against a group is punishable by a fine of 200 Bahraini dinars and up to years' imprisonment if such incitement disturbs the public peace.

On January 4, 2019, the United Nations High Commissioner for Human Rights issued a statement criticising a five-year prison sentence for prominent

human rights defender Nabil Rajab for "spreading false news and rumours in times of war", "insulting foreign countries" and "publicly insulting the Ministry of Interior". Rajab has been imprisoned in Bahrain since July 2016 for posting tweets in 2015 about Saudi airstrikes in Yemen and allegations that he was tortured in Jaw prison in Bahrain. "We have the right to say no to the war in Yemen, and we must fight for peace and security, not for bloodshed in Sanaa," he tweeted. Bahrain's highest judicial body – the Court of Cassation – upheld Rajab's conviction and five-year sentence. In 2018, the United Nations Working Group on Arbitrary Detention found that Rajab's detention was arbitrary.⁵⁶

⁵⁶ "Briefing note on Bahrain," Office of the UN High Commissioner for Human Rights, January 4, 2019, <https://www.ohchr.org/AR/NewsEvents/Pages/DisplayNews.aspx?NewsID=24055&LangID=A;>

The penalties are high for contravening Saudi Arabia's publishing laws, in particular the Press and Publications Law (amended in 2011), the Electronic Publishing Regulations and the Cybercrime Law. The law provides a shield of immunity to "members of the Senior Scholars, Statesmen or any of its employees," as stipulated in Article 7 of the Saudi Press and Publications Law.⁵⁷ If the violation constitutes an offense against the Islamic religion or affects the interests of the state, it is referred for submission to the king to consider legal procedures such as filing the lawsuit before the competent court, or taking whatever action the king deems in the public interest.

The Saudi Press and Publications Law prohibits the publication of anything that would prejudice the country's security or public order, or that serves foreign interests that are contrary to the national interest. It also forbids publication of material that would defame, insult or damage the reputation or dignity of the Grand Mufti of Saudi Arabia or members of the Council of Senior Scholars or Statesmen, any of its employees or any person. Finally, inciting strife and

spreading division among citizens or undermining the public interest is criminalised.

Whoever violates the provisions of this Law is liable to one or more of the following penalties:

- A fine not exceeding 500,000 Riyals (about USD145,000), which is doubled for repeat offences.
- A ban on the offender from writing in any newspapers or publications, or participating in broadcast media.
- The temporary or permanent closure of the place of the violation.

If the violating entity is a newspaper, the decision to close it shall be executed with the approval of the prime minister. If the place of the violation is an electronic newspaper or a website, the execution of the closure or blocking decision shall be pursuant to the decision of the competent minister.

The new electronic publishing regulations in Saudi Arabia also prohibit the publication of anything calling for disturbing the country's security or

public order, serving foreign interests contrary to the national interest, inciting criminal activity, inciting hatred, spreading obscenity, or encouraging racial discrimination between members of society.⁵⁸

Under the Cybercrime Law,⁵⁹ infringing on privacy by misusing camera phones and defaming or harming others using information technology is punishable by imprisonment for up to a year and a fine of up to 500,000 Saudi riyals.

The following offenses are punishable by a term of up to five years' imprisonment and a fine of up to 3 million Saudi riyals (approx. USD850,000):

- Producing, preparing, transmitting or storing information through a computer or a computer network that may prejudice public order, religious values, public morals or the sanctity of private life.
- Creating a website to facilitate human

trafficking.

- Creating, disseminating or promoting of materials related to pornography or gambling that disrupts public morals.
- Establishing or disseminating a website to promote the trafficking or use of drugs and psychotropic substances.

The following offenses are penalised by up to 10 years' imprisonment and up to 5 million Saudi riyals:

- Creating or publishing a website or using a computer to facilitate communication with the makers of incendiary devices, explosives, or any tool used in terrorist acts.
- Illegal access to a website or access to an information system through the Internet or a computer to obtain data affecting the internal or external security of the State or its national economy.

⁵⁸ "Regulations for electronic publishing activity," Saudi Arabia Ministry of Media, <https://www.media.gov.sa/page/74>

⁵⁹ "Anti-Cyber Crime Law," Communications and Information Technology Commission, <https://www.citc.gov.sa/en/RulesandSystems/CITCSYSTEM/Pages/CybercrimesAct.aspx>

Sultanate of Oman

The Cybercrime Law⁶⁰ No. 12 of 2011 criminalises infringement of the integrity and confidentiality of data and information belonging to the government, banks and financial institutions. It also prohibits the circulation of pornographic material; incitement to commit “debauchery” or prostitution; threats or extortion; publication of terrorist ideology; the dissemination of methods to manufacture explosives and weapons; money laundering; illicit trafficking in antiquities; copyright infringement; violation of the sanctity of the private or family life of individuals; breach of public morals; and promotion of programmes, ideas or activities that lead to such acts.

The law tightens sanctions for drug trafficking. Creating a website, spreading information online or using information technology to traffic or promote drugs is punishable by death or absolute imprisonment (life imprisonment as in previous laws but usually 25 years) and a fine of between 25,000 and 100,000 Omani rials (approx. USD 65,000 to USD 250,000).

Several social media activists have been arrested for criticising normalisation with Israel.⁶¹

Qatar

Qatar’s Cybercrime Law No. 14 of 2014⁶² criminalises anyone who establishes or operates a website for a terrorist group or organisation or promotes terrorist ideas, finances terrorism, or publishes information about how to manufacture incendiary or explosive devices online or on any information technology medium.

It prohibits the publication of false news with intent to endanger the safety, public order, internal or external security of the State. It also criminalises the transmission or possession of pornographic material involving minors by means of information technology. Further, it prohibits the violation of the sanctity of private or family life, defamation, blackmail and extortion through the Internet or any medium of information technology.

⁶⁰ “Information Technology Crime Law,” Ministry of Technology and Communications, April 11, 2011, https://www.ita.gov.om/ITAPortal_AR/MediaCenter/Document_detail.aspx?NID=64

⁶¹ “Omani security arrests activists who criticised normalisation with Israel,” Arabic 21, February 19, 2019, <https://m.arabi21.com/story/1161198>

“Omani Internal Security Arrests Social Media Activists,” Skyline International, February 20, 2019, <https://skylineforhuman.org/en/omani-internal-security-arrests-social-media-activists-2/>

⁶² Cybercrime Law No. 14 of 2014, Qatar Ministry of Interior, <https://portal.moi.gov.qa/wps/wcm/connect/7a95aa55-3143-4c86-9279-6d57a1f54301/لأ نون+بإصدار+قانون+مكافحة+الجرائم+الإلكترونية.pdf?MOD=AJPERES>

The Cybercrime Act of 2007 in Sudan⁶³ shares most of the common factors of the Arab legislation described above, but it is unique in several articles, including the following:

Article 14: Whoever produces, prepares, sends, stores, or promotes any content that is offensive to public order or morality through the Internet or a computer shall be punished by up to five years' imprisonment and/or a fine to be determined by the court. (Article 34 of the Sudanese Criminal Code states that the court shall assess the fine in view of the nature of the crime committed, the amount of ill-gotten acquisition and the degree of involvement of the offender and their financial situation. The court may order the partial or full payment of the fine as compensation to the victim of the crime.) Any person who intentionally or negligently provides, through the Internet, a computer or the like, access to content that is indecent and contrary to public order or morality shall be punished by imprisonment for up to four years, or by a fine, or both.

Article 15: Any person who creates, publishes or uses a website, a computer or the like to facilitate or promote

programs or ideas contrary to public order or morality shall be punished by imprisonment for a term not exceeding three years, or by a fine, or both.

Article 16: Any person who violates or offends any religious belief or the sanctity of private life through the Internet, a computer or the like shall be punished by imprisonment for up to three years, a fine, or both.

Article 17: Any person who uses the Internet, a computer or the like to harm the reputation of another shall be punished by imprisonment for up to two years, or by a fine, or both.

Article 19: Any person who unlawfully publishes through the Internet, a computer or the like, any intellectual or literary works, scientific research or the like shall be punished by imprisonment for up to one year, a fine, or both.

In June 2018, the Sudanese parliament passed a draft cybercrime law to replace the 2007 cybercrime law. Due to current events in Sudan, it is not expected to be a priority for legislators.

⁶³ "Cybercrime Act, 2007," Available at UN Office on Drugs and Crime, https://www.unodc.org/res/cld/document/sdn/2007/cybercrime_act_2007.html/Sudan_Cybercrime_Act_2007_EN.pdf

Syria

Syria's Legislative Decree No. 17 of 2012 penalizes anyone who incites or promotes crimes through computer networks.⁶⁴

Article 23 states that whoever disseminates through the network information that violates the privacy of any person without his consent, even if such information is true, shall be punished by imprisonment from one to six months and a fine of 100,000 to 500,000 Syrian pounds.

Article 32 states that the Network shall be one of the public means provided for in the Penal Code and the penal laws in force.

In March 2018, new anti-cybercrime legislation was passed in Syria, creating special courts of first instance for cybercrimes.⁶⁵

Algeria

Law No. 09-04 legislates the prevention and control of offenses related to information and communication technologies.⁶⁶

Article 4 of the law allows the monitoring of communications related to the prevention of terrorist acts and attacks on state security without prejudice to the private life of others.

Article 12b states that ISPs shall make arrangements to restrict access to subjects that contain information contrary to public order or morals and shall inform their subscribers of their existence.

⁶⁴ "Legislative decree 17 of 2012," Parliament of Syria, February 8, 2012, <http://www.parliament.gov.sy/arabic/index.php?node=201&nid=4337&ref=tree&>

⁶⁵ "Syrian Government Passes New Anti-Cybercrime Bill," SMEX, March 14, 2018, <https://smex.org/syrian-government-passes-new-anti-cybercrime-bill/>

⁶⁶ Published in the Official Gazette, August 16 2009, No. 47 p.5. https://www.arpce.dz/ar/doc/reg/loi/Loi_09-04.pdf.

Mauritania

Law No. 2016-007 on Cybercrime⁶⁷ is in line with most Arab laws in criminalising pornography, especially if it is directed against children, and prohibiting infringement of privacy and dissemination of secrets related to defence and national security.

Issues of race and discrimination are politically sensitive in Mauritania. Article 1 of the Constitution states: “Any regional propaganda of a racial or ethnic nature shall be punished by law.”

Article 21 of the cybercrime law states that transmission or dissemination of a text message, image, sound or any other form of audio-visual representation that affects the values of Islam is punishable with imprisonment of one to four years and a fine of 200,000 to 3 million ouguiya.

Article 22 criminalises insulting a person or a group on the basis of their race, colour, descent, national or ethnic origin with punishments of imprisonment from one month to one year and/or a fine of 300,000 to 2 million ouguiya, without prejudice to compensation for the damage caused to the victim.

Article 23 states that whoever intentionally, through an information system, produces, registers, displays, provides or disseminates a text message, image, voice or any other form of presentation of ideas and theories that glorifies crimes against humanity or incites violence and/or racial hatred shall be punished by imprisonment from one month to one year and/or fined between 200,000 to 2 million ouguiya, without prejudice to compensation for the damage caused to the victim.

⁶⁷ Law No. 2016-007 on Cybercrime published in the Official Gazette of the Republic of Mauritania on February 29, 2015 p.1354. <http://www.tic.gov.mr/IMG/pdf/loi2016007cybercrimemar.pdf>.

Although the Tunisian cabinet approved a draft law on combating crimes related to information and communication systems in mid-2018, the parliament has yet to discuss the bill. Therefore, there is no uniform law dealing with cybercrime in Tunisia. Despite leading the Arab Internet Freedom Index in 2018, Tunisia has enacted several restrictive laws since the overthrow of former President Zine El Abidine Ben Ali. Some argue that there is no need to enact a law to regulate online publishing because the general rules govern the dissemination of published content, whatever the means of publishing used.

The following are relevant legal articles:

Organic law no. 26 dated 7 August 2015, on combating terrorism and preventing money laundering⁶⁸:

Chapter 14 of law no. 26 lists a number of acts as terrorist offenses, including declaring someone a disbeliever or advocating or inciting hatred or animosity between races, religions and doctrines, which is punishable by imprisonment of one to five years and a fine of 5,000 to 10,000 Tunisia dinars.

Chapter 34 states that providing, by any means, materials, equipment, means of transport, equipment, supplies, websites, documents or photographs for a terrorist organisation or for persons connected with terrorist offenses is punishable by imprisonment of 10 to 20 years and a

fine of 50,000 to 100,000 Tunisian dinars.

Organic law no. 50 dated 23 October 2018, on the elimination of all forms of racial discrimination⁶⁹:

Chapter 2 of this law defines racial discrimination as any distinction, exclusion, restriction or preference based on race, colour, descent, national or ethnic origin or other forms of racial discrimination based on ratified international treaties, which would result in deprivation of the enjoyment of rights and freedoms or additional burdens.

Chapter 9 states that the following acts are punishable by imprisonment from one to three years and a fine of 1,000 to 3,000 Tunisian dinars (approx. USD350-1,050):

- Incitement to, or threat of, hatred, violence, discrimination, segregation, or threats against a person or group of persons on the basis of racial discrimination.
- Disseminating ideas based on racial discrimination, racial superiority or hatred by any means.
- Commending the practices of racial discrimination through any means.
- Forming a group or organisation that explicitly and repeatedly supports racial discrimination or membership or participation in it.
- Supporting or financing activities, associations or organisations of a racial nature.

⁶⁸ "Organic Law no 26 of 2015, dated August 7, 2015, on combating terrorism and preventing money laundering," National Portal of Legal Information - Republic of Tunisia, http://www.legislation.tn/detailtexte/Loi-num-2015-26-du-07-08-2015-jort-2015-063__2015063000261.

⁶⁹ "Organic Law no 50 of 2018, dated October 23, 2018, on the elimination of all forms of racial discrimination," National Portal of Legal Information - Republic of Tunisia, http://www.legislation.tn/detailtexte/Loi-num-2018-50-du-23-10-2018-jort-2018-086__2018086000501.

Morocco

There is no uniform law in Morocco for cybercrime or crimes committed through information systems. However, criminal acts are divided into several laws, the most important of which is the Moroccan Criminal Code which criminalises accessing data processing systems through fraud; attacks on data and information stored on a computer through fraud, forgery or theft; and obtaining such data and information without permission or through fraudulent means.

Iraq

There is no law in Iraq specialised in dealing with cybercrime⁷⁰, although a law on cybercrimes has been submitted by the House of Representatives pending legislation. In the meantime, Iraqi authorities deal with cybercrimes under the Iraqi Penal Code No. 111 of 1969 as amended, the Anti-Terrorism Law and other legislation.

In February 2015, the first judicial decree criminalising defamation on Facebook was issued by the Baghdad Court of Appeal of Rusafa. Penal Resolution 989 of 2014 stated that the social media platform Facebook was a public medium⁷¹ and that the dissemination of libelous expressions through the platform constituted publication through one of the means of publicity. This requires a harsher punishment for the perpetrator, since Facebook pages are available to the public. In this decision, the Iraqi judiciary recognised an important principle when it considered Facebook as a public forum.

⁷⁰ Dr Laila Janabi (2017). The Effectiveness of National and International Laws in Combating Cyber Crimes p.11.

⁷¹ Article by Judge Iyad Mohsen Dhamd: Defamation via Facebook.

In Lebanon, there is also no law that deals with cybercrime; libel and slander crimes committed online and on social media are dealt with in accordance with the general rules of the Lebanese Penal Code. The text of Article 209 on Publicity was amended by Electronic Transactions and Personal Data Law⁷² (the E-transaction law) No. 81 of 2018 (issued on October 10, 2018) to cover the following aspects: "Writing, drawings, paintings, photographs, films and signals, of any kind, if presented in a public place or a permitted place, sold, offered for sale or distributed to one or more persons, regardless of the means, including electronic means."

Under the Transactions and Personal Data Law, crimes against morals and public morals were also amended by Decree No. 340 of 1/3/1943 (Penal Code). Penalties were replaced by the following provisions (Section 3) for crimes of exploitation of minors in pornography:

Article 535: Exploitation of minors in pornography means filming, showing or distributing tangible representation of any minor by any means. This includes

drawings, pictures, writings, films or signs, and also includes the practice of real or artificial explicit sexual activities or any depiction of the genital organs of a minor.

The provisions of the Penal Code shall apply, where the conditions are met, to criminal offenses related to the exploitation of minors in pornography, subject to the provisions of the following article.

Article 536: The preparation or production of pornographic material involving the active participation of minors, relating to the exploitation of minors in pornography, is considered as a crime of trafficking in persons, and the perpetrator is punished in accordance with the provisions of Article 586 et seq. of the Penal Code relating to trafficking in persons.

The law is clearly influenced by European guidelines and the Budapest Convention on Cybercrime.

Yemen

Yemen has no cybercrime law. Cyber offenses are dealt with by the general rules of the Penal Code and other relevant laws. Yemeni lawyer Ahmad Arman⁷³ said: “In general, for cybercrime, it can be said that Yemeni law, whether the law of crimes and penalties, or any of the provisions of criminalisation and punishment in various laws, including the press and publications law, lacks clear provisions on cybercrime. In some cases, some courts have applied general provisions in the face of cases concerning freedom of expression.”

⁷³ Correspondence with the researcher on April 17, 2019.

.3

A comparison between the laws of cybercrime in the Arab countries

Most cybercrime laws in Arab countries (and a number of other countries) agree on criminalising the following acts:

1. Illegal access to any information system or network for the purpose of changing data or information.
2. Disabling any website or electronic service.
3. Protection of correspondence and communications of individuals.
4. Dissemination of child pornography.
5. Forging an electronic signature.
6. Seizure of money (or credit card data) using fraudulent methods.
7. Trafficking in persons.
8. Drug trafficking.
9. Money-laundering
10. Gambling
11. Terrorism and the promotion or financing of the terrorist ideology or the dissemination of information on how to manufacture incendiary or explosive devices.
12. Obtaining confidential government information.

The Arab Convention on Combating Technology Offences⁷⁴ is an attempt to unify cybercrime legislation. Most Arab countries signed⁷⁵ this Convention on December 21, 2010 (except Lebanon, Djibouti, Somalia and Comoros) and six Arab states have ratified or acceded to it. According to the text of its fifth chapter, the Convention comes into force after the ratification of seven Arab countries, which has not yet been achieved.

The Convention criminalises “access to confidential government information” (Art. 6.2.b). It also criminalises the production or transmission of pornographic or indecent material, particularly relating to children. It criminalises terrorism-related offenses committed by information technology such as inciting strife and sedition or assaulting religions and beliefs. It also prohibits money-laundering, copyright infringement, illegal use of electronic payment tools and trafficking in people, organs, drugs or illicit arms.

The Convention uses general terms and contains no clear definition of what constitutes “indecent” material; it can therefore be used to criminalise many types of content published on the Internet, whether literary or artistic, or any digital content.⁷⁶

⁷⁴ “Arab Convention on Combating Technology Offences,” Available at: Jordanian Ministry of Justice, <http://www.moj.gov.jo/EchoBusV3.0/SystemAssets/27adcb7a-5539-4b36-9d9a-28b91f578bac.pdf>

⁷⁵ Signature of the convention means the goodwill of the State to give effect to the Convention and to incorporate it into national legislation to be ratified.

⁷⁶ Mohammad Al-Taher, “Comment on The Arab Convention on Combating Technology Offences,” AFTE Egypt, March 12, 2015, https://afteegypt.org/digital_freedoms/2015/03/11/9770-afteegypt.html.

The Economic and Social Commission for Western Asia (ESCWA) has already developed guidelines for cyber legislation,⁷⁷ designed to assist Arab countries in developing and harmonising national cyber laws at the regional level. Since 2009, ESCWA has been implementing the cyber legislation harmonisation project to strengthen and harmonise cyber and ICT legislation in the Arab region.

The Guidelines provide proposals to criminalise racism and practices against humanity committed by electronic means,⁷⁸ such as distributing information by electronic means that would deny, distort, justify, assist or incite acts of genocide or crimes against humanity. They also propose criminalising the dissemination and distribution of information that incites conflict aiming at racial discrimination against certain persons, and threatening, humiliating or abusing persons because of their ethnic or sectarian affiliation or colour through the Internet, or by any means of information technology.

It should be noted that two Arab states (the UAE and Tunisia) have criminalised past acts if committed by electronic means.

Cybercrime laws in the following Arab countries are unique in criminalising certain acts:

| Criminal acts | Jordan | Kuwait | Egypt | Oman | UAE | Bahrain |
|--|---------------|---------------|--------------|-------------|------------|----------------|
| Violation of the privacy of individuals | Yes | | Yes | | | |
| Threat or extortion | Yes | Yes | | | Yes | Yes |
| Violation of public morals | Yes | | Yes | | | |
| Prostitution or debauchery | Yes | Yes | | | Yes | No |
| Gambling | Yes | | | | Yes | No |
| Publication of confidential government information | Yes | Yes | Yes | | Yes | No |
| Libel and slander | Yes | | | Yes | Yes | |
| Dissemination of incorrect news or rumours | Yes | | | | Yes | |
| Incitement to hatred | Yes | | | | Yes | |
| Abusing the prestige of the state or its institutions and symbols | Yes | | | | Yes | |

⁷⁷ "Guidance of ESCWA for cyber legislation," UNESCWA, 2012, https://www.unescwa.org/sites/www.unescwa.org/files/page_attachments/directives-full.pdf

⁷⁸ Ibid, p. 134, Articles 34-37.

CHAPTER 3

International Standards for Freedom of Opinion and Expression on the Internet and their Legal Restrictions



Freedom of expression is not absolute in any jurisdiction; restrictions may be imposed according to international standards, in particular the International Covenant on Civil and Political Rights (ICCPR)⁷⁹, which is a binding international convention. The Covenant has been ratified by 172 countries, including most Arab states (except Saudi Arabia, the UAE and Oman)⁸⁰. The provisions of the Covenant take precedence over national laws in the event of conflict.

A key challenge is finding a balance between the protection of freedom of expression and the protection of public interests (especially national security and public morals) and private interests that may be threatened when this freedom is abused. Many mistakenly believe that the Internet is a free zone for defamation (libel and slander). As a result of this misunderstanding, they risk imprisonment, a fine (to the state), payment of compensation to the victim and other sanctions. It is also a common misperception that the law does not apply to posts on Facebook and Twitter; this fails to recognise that these are public platforms and therefore posts to them can constitute libel or slander.

Restrictions on freedom of expression can be divided into two parts:

1. Optional restrictions, as in Article 19 of the International Covenant on Civil and Political Rights.⁸¹
2. Obligatory restrictions, as in Article 20 of the Covenant⁸² and the Convention on the Prevention and Punishment of the Crime of Genocide (1951) and the Convention on the Elimination of All Forms of Racial Discrimination (1969).

The free flow of information must always be the rule, not the exception.⁸³ Every restriction that limits dialogue must be carefully weighed to ensure that it remains exceptional and that legitimate discourse is not prohibited.

For the restriction to be lawful, the elements of the three-part test derived from the third paragraph of Article 19 of the Covenant must apply:

- The restriction shall be exceptional via a provision of the law (not arbitrary) and not to expand it as it is necessary in a democratic society (the restriction shall be the last resort).

⁷⁹ Adopted by the United Nations General Assembly in Resolution 2200A (XXI), December 16, 1966, entered into force March 23, 1976. See: "International Covenant on Civil and Political Rights," United Nations Treaty Collection, https://treaties.un.org/doc/Treaties/1976/03/19760323%2006-17%20AM/Ch_IV_04.pdf

⁸⁰ "International Covenant on Civil and Political Rights," United Nations Treaty Collection, https://treaties.un.org/Pages/ViewDetails.aspx?chapter=4&clang=en&mtdsg_no=IV-4&src=IND

⁸¹ Article 19 stipulates:

1. Everyone shall have the right to hold opinions without interference.
2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

(a) For respect of the rights or reputations of others;

(b) For the protection of national security or of public order (order public), or of public health or morals.

⁸² Article 20. 1. Any propaganda for war shall be prohibited by law. 2. Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law.

⁸³ "Countering online hate speech," UNESCO, 2015, <https://unesdoc.unesco.org/ark:/48223/pf0000233231>

Within the interpretations of the European Court of Human Rights, “necessity” means the existence of “pressing social need” and intervention shall be “proportionate to the legitimate aim pursued”.⁸⁴

- To protect a legitimate objective, not a show of force (such as criminalising government criticism and immunising officials from criticism).
- Public interest overrides if it conflicts with the right to privacy. For example, it is not permissible to publish any indication that an official has diabetes because the private interest prevails here, but if the official has an infectious disease or it affects the performance of his work, the public interest will prevail.

General Comment 34 of the Human Rights Committee⁸⁵ of 2011, which monitors the application of the International Covenant on Civil and Political Rights, states that when restricting freedom of opinion and expression based on Article 20, the restriction must be consistent with the three-part test. It also stipulates that restrictions on the Internet should not exceed legitimate restrictions when freedom of expression is practiced offline (by old methods before the birth of the Internet).⁸⁶ The limitations should be clear and specific, necessary and proportionate to the interest to be protected.

Prosecution for peaceful criticism of public

officials violates international human rights standards. Officials must tolerate criticism more than ordinary citizens. This distinction serves the public interest because it makes it difficult to prosecute criticism of public officials and public figures. The UN Human Rights Committee has expressed concern about laws on issues of disrespect for power, lack of respect for state flags and state symbols and prohibition of criticism of government institutions.⁸⁷

In 2012, the UN Human Rights Council adopted a landmark resolution that “the same rights of those persons who are not online to the Internet must also be protected online”.⁸⁸

Article 32 of the Arab Charter on Human Rights⁸⁹ states:

1. This Charter guarantees the right to information and freedom of opinion and expression, as well as the right to receive and impart information and ideas through any media and regardless of geographical boundaries.
2. These rights and freedoms shall be exercised within the framework of the basic elements of society and shall be subject only to restrictions imposed by respect for the rights or reputations of others or the protection of national security, public order, public interest or morals.

⁸⁴ Clayton, R. and Tomlinson, H. (2000). *The Law of Human Rights*, Oxford University Press. p.1058.

⁸⁵ “General comment no. 34,” International Covenant on Civil and Political Rights, UN Human Rights Committee, September 12, 2011, <https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>

⁸⁶ *Ibid*, paragraph 12.

⁸⁷ *Ibid*, paragraph 38.

⁸⁸ “The promotion, protection and enjoyment of human rights on the Internet,” United Nations Human Rights Council, July 16, 2012 (A/HRC/RES/20/8), http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/20/8

⁸⁹ The Arab Charter for Human Rights entered into force on January 24, 2008. Available in Arabic: <http://www1.umn.edu/humanrts/arab/a003-2.html>

.1

Balancing the protection of privacy and national security, including the prohibition of discriminatory discourse and the protection of freedom of expression

Freedom of expression can lead to conflict with other rights such as the right to privacy.⁹⁰ The Egyptian Court of Cassation says in this regard that when two interests conflict, the law “balances two rights; one is wasted to preserve the other.”⁹¹

Protection of privacy

Article 17.1 of the International Covenant on Civil and Political Rights stipulates that: “No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.”

Article 12 of the Universal Declaration of Human Rights⁹² stipulates that: “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”

Arab laws fail to criminalise certain dangerous behaviours on the Internet and social media such as cyberbullying⁹³ and aggressive behaviour aimed at fear-mongering.

The Declaration on Media Freedom in the Arab World⁹⁴ calls on “politicians and public figures to tolerate a higher degree of criticism than ordinary citizens; with the right to prove allegations against them in cases of concern to citizens.” The declaration states: “Efforts should be made to spread the culture of informatics and communication among citizens, and this includes social media education.”

⁹⁰ Dr Mohammed Yousef Alwan and Dr. Mohammed al-Mousa, *International Human Rights Law*, Dar al-Thaqafa, vol. 2, p.285.

⁹¹ Nasrameen, *The Egyptian Judicial System*, Amin Law Firm 2004, p.74.

⁹² “The Universal Declaration of Human Rights,” United Nations, <https://www.un.org/en/universal-declaration-human-rights/>

⁹³ Sarah Jameson, “Cyber Harassment: Striking a balance between free speech and privacy,” p. 236. *CommLaw Conspectus*, Vol. 17, 2008, <https://scholarship.law.edu/cgi/viewcontent.cgi?article=1403&context=commlaw>

⁹⁴ Palestine was the first country to sign the declaration on August 2, 2016, followed by Tunisia on August 26, 2018, Jordan on October 12, 2016, Sudan and finally Kuwait. The announcement was the culmination of 20 months of consultations, with the participation of international and regional experts and media actors. It was finalised at a conference organised by the International Federation of Journalists (IFJ) in Casablanca on May 3, 2016 with the support of a number of international organisations, including UNESCO, and the EU-funded Meydan project.:

Protection of national security

Article 19 of the ICCPR allows for restrictions on freedom of expression to protect national security. The Johannesburg Principles⁹⁵ are among the most important and best criteria for balancing freedom of expression and national security. Discussing the grounds for a restriction to be lawful and in the interest of national security, the Johannesburg Principles state: "A restriction sought to be justified on the ground of national security is not legitimate unless its genuine purpose and demonstrable effect is to protect a country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force, whether from an external source, such as a military threat, or an internal source, such as incitement to violent overthrow of the government. In particular, a restriction sought to be justified on the ground of national security is not legitimate if its genuine purpose or demonstrable effect is to protect interests unrelated to national security, including, for example, to protect a government from embarrassment or exposure of wrongdoing."⁹⁶



⁹⁵ The Johannesburg Principles on National Security, Freedom of Expression and Access to Information are accredited by a team of experts in international law and national security and human rights dated October 1, 1995 under Article 19, in cooperation with the Centre for Applied Legal Studies at the University of Witwatersrand and University of Johannesburg. See: "The Johannesburg Principles on National Security. Freedom of Expression and Access to Information," Article 19, November 1996, <https://www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf>

⁹⁶ Ibid, Principle 2.

Prohibition of discriminatory discourse

As mentioned above, Article 20 of the Covenant imposes on member states a positive obligation to intervene to prohibit discriminatory discourse and any call for national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence.

One of the best international standards for locating the line between freedom of expression and incitement to discriminatory discourse is the **Rabat Plan of Action** on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence.⁹⁷ Introducing the plan in Geneva in February 2013, UN High Commissioner for Human Rights Navi Pillay said: “In recent years, incidents involving hate speech, negative stereotyping in the media, and even advocacy of religious or national hatred by public officials and political parties have resulted in killings of innocent people, attacks on places of worship and calls for reprisals.” She added: “This spiral of violence has made it incumbent on us to renew the search for the correct balance between freedom of expression – which is among the most precious and fundamental of our rights as human beings – and the equally vital need to protect individuals and communities from discrimination and violence.”⁹⁸

The Rabat Plan of Action states that hate expression must be criminalised if it passes

a six-part test: Context, speaker, intention, content, extent of discourse, and likelihood of harm.

Article 4 of the International Convention on the Elimination of All Forms of Racial Discrimination⁹⁹ stipulates that: “State Parties condemn all propaganda and all organisations which are based on ideas or theories of superiority of one race or group of persons of one colour or ethnic origin, or which attempt to justify or promote racial hatred and discrimination in any form, and undertake to adopt immediate and positive measures designed to eradicate all incitement to, or acts of, such discrimination.”

The Declaration on Media Freedom in the Arab World¹⁰⁰ states that hate speech and intolerance¹⁰¹ must be prohibited and that the media bears professional, moral, and social responsibility in combating hatred, intolerance and sectarianism. The Declaration urges “exerting efforts to spread the culture of information and communication among citizens, including education on the subject of dealing with social networks.”¹⁰²

At UNESCO’s ceremony for World Press Freedom Day in Ghana on May 2, 2018, rapporteurs for freedom of expression at the United Nations, Europe, the Americas and Africa issued a joint declaration on the independence and diversity of media in the digital age.¹⁰³

⁹⁷ The Rabat Action Plan is the product of several regional meetings in which three UN Special Rapporteurs participated: Frank Iaro, Special Rapporteur on freedom of opinion and expression; Heiner Bielefeldt, Special Rapporteur on freedom of religion or belief; the Special Rapporteur on the question of racism, racial discrimination, xenophobia and related intolerance, Motoma Rotiri, along with Anis Kalamar, Executive Director of Article 19, as well as 45 experts from different cultural backgrounds and legal traditions. See: “Annex - Annual Report of the UN High Commissioner for Human Rights,” UN Human Rights Council, January 11, 2013, https://www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome.pdf

⁹⁸ “Annex - Annual Report of the UN High Commissioner for Human Rights,” UN Human Rights Council, January 11, 2013, https://www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome.pdf

⁹⁹ Adopted and submitted for signature, ratification and accession by General Assembly resolution 2106 of 21 December 1965, date of entry into force: 4 January 1969, in accordance with article 19: “International Convention on the Elimination of All Forms of Racial Discrimination,” UN Office of the High Commissioner for Human Rights, <https://www.ohchr.org/en/professionalinterest/pages/cerd.aspx>

¹⁰⁰ “Declaration on Media Freedom in the Arab World,” International Federation of Journalists, <http://www.ifj-arabic.org/page-ifj-645.html>

¹⁰¹ *Ibid.*, principle 8. ¹⁰² *Ibid.*, principle 4b. ¹⁰³ “Joint declaration on media independence and diversity in the digital age,” UN Office of the High Commissioner for Human Rights, May 3, 2018, https://www.ohchr.org/Documents/Issues/Opinion/JointDeclaration2May2018_EN.pdf

.2

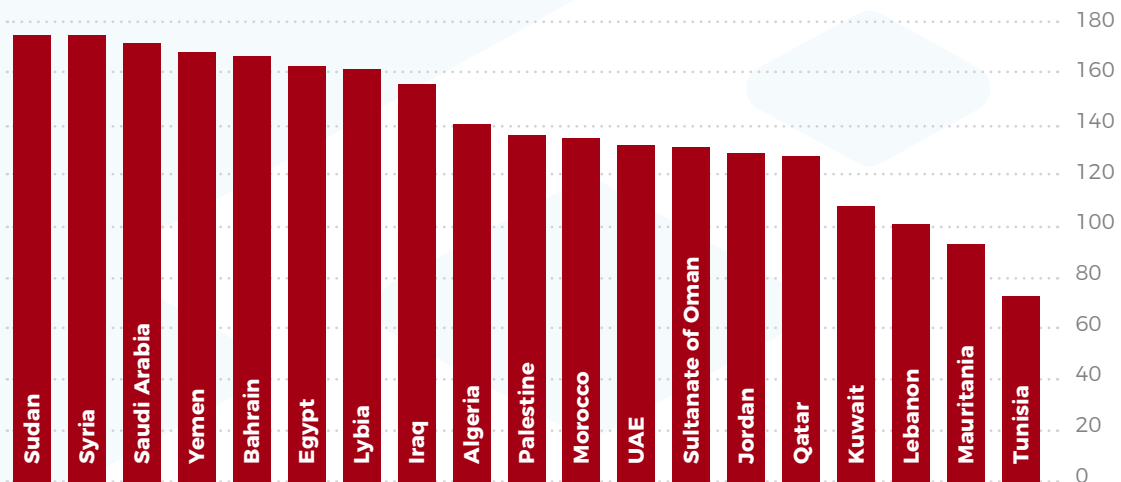
Freedom of the press and media in the Arab countries

As evidenced above, when international standards of freedom of opinion and expression are compared with Arab cybercrime laws, most of the latter's provisions do not comply with the standards of legitimate restrictions, instead hindering dialogue and curbing freedom of expression.

Below is a map that illustrates the world's press freedom by Reporters Without Borders for 2019. The index measures press freedom in 180 countries (black: very serious situation; red: difficult situation; orange: problematic situation; yellow: satisfactory situation; white: good situation).¹⁰⁴



¹⁰⁴ "Ranking - 2019 World Press Freedom Index," Reporters Without Borders, <https://rsf.org/en/ranking>



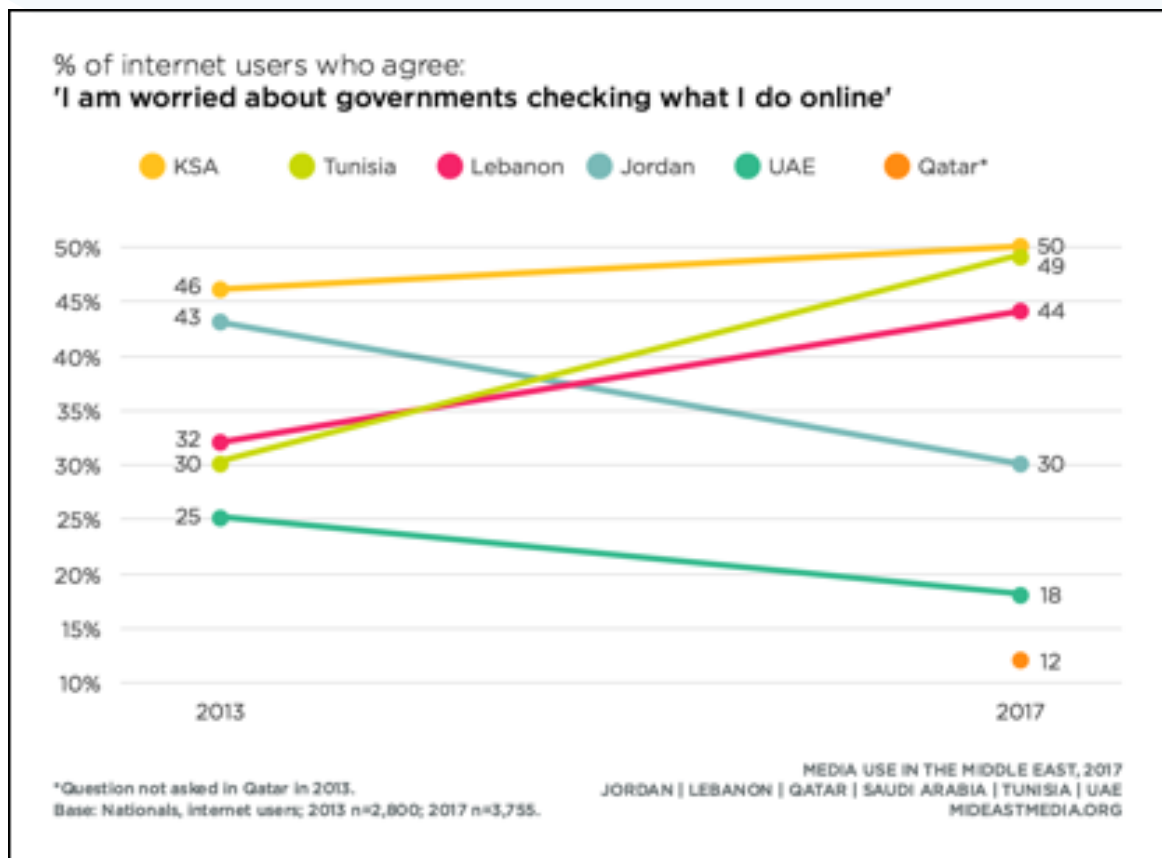
Reporters Without Borders 2019 press freedom index, which measures the freedom of the press in 180 countries (the lowest number is most free and the highest (180) is least free)¹⁰⁵

The following table shows the ranking of Arab countries in the annual Internet Freedom index according to Freedom House. The lowest scores represent countries with the most freedom and the highest represent countries with the least freedom. It consists of three categories: Free, partially free, and not free.¹⁰⁶ As noted from the previous index, no Arab country falls in the “free” category of the index.

| Country | In 2018 | | In 2017 | | Change +/- |
|---------|---------|----------------|---------|----------------|------------|
| Jordan | 49 | Partially free | 53 | Partially free | + 4 |
| Bahrain | 71 | Not free | 72 | Not free | +1 |
| Lebanon | 47 | Partially free | 46 | Partially free | - 1 |
| Tunisia | 38 | Partially free | 38 | Partially free | 0 |
| Morocco | 45 | Partially free | 45 | Partially free | 0 |
| Egypt | 72 | Not free | 68 | Not free | - 4 |
| Saudi | 73 | Not free | 72 | Not free | - 1 |
| UAE | 69 | Not free | 69 | Not free | 0 |
| Syria | 83 | Not free | 86 | Not free | + 3 |
| Sudan | 65 | Not free | 64 | Not free | - 1 |
| Libya | 51 | Partially free | 54 | Partially free | + 3 |

¹⁰⁵ The table is prepared by the researcher based on the RSF index. "Ranking - 2019 World Press Freedom Index," Reporters Without Borders, <https://rsf.org/en/ranking>

¹⁰⁶ "Freedom on the Net 2018 Map," Freedom House, <https://freedomhouse.org/report/freedom-net/freedom-net-2018/map>



A survey shows the extent of fear from governments in tracking what citizens are doing online ¹⁰⁷

Blocking websites

As previously mentioned, Article 20 of the International Covenant on Civil and Political Rights requires State parties to intervene to prohibit discriminatory discourse and any call for national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence. In accordance with international standards, “any restrictions on the operation of websites, blogs or other online or electronic means or any other information dissemination system, including support systems for such communications, are only permitted if such means are to some extent compatible with Article 19, paragraph 3, of the Covenant.”¹⁰⁸ Blocking websites also violates the rights of those wishing to access information. In exceptional circumstances, blocking websites can be the last option if there is no other less intrusive way of addressing the damage, such as deleting controversial content.

The reasons for blocking websites vary in many countries in order to prevent the

promotion of pornography, especially with regard to children, gambling, drugs and illegal content. An example of violating international standards is the blocking of websites in Jordan simply because the site has not been licensed.¹⁰⁹ In Egypt, the site must be licensed if the number of its followers exceeds 5,000, otherwise it will be blocked, especially if it publishes content that is contrary to the government’s agenda.

Arab countries and other ISPs are demanding that certain materials be banned, which may constitute a kind of privatisation of content-censorship. In the UAE, for example, an ISP should ban unethical and sensitive political material and any content that is contrary to public morality.¹¹⁰

In Yemen, licensed ISPs are prohibited from accessing sites that fall into the categories of gambling, sexual content and any material that seeks to convert Muslims to other religions.

¹⁰⁸ General Comment No. 34: Article 19: Freedom of Opinion and Expression, paragraph 43; “Freedom of Expression Unfiltered: How blocking and filtering affect free speech,” Article 19, December 8, 2016, <https://www.article19.org/resources/freedom-of-expression-unfiltered-how-blocking-and-filtering-affect-free-speech/>

¹⁰⁹ The Media Commission blocks 45 news websites.

¹¹⁰ ESCWA (2007). Examples of cyberspace legislation in ESCWA member countries, p.23.

CONCLUSION & RECOMMENDATIONS



Conclusion

- 1.** It is clear from the foregoing that there are provisions in a number of Arab cybercrime laws referred to in this paper that are incompatible with international treaties and conventions, resulting in a conflict in practical application.
- 2.** Legislation tends to tighten penalties, which goes beyond the principle of proportionality of the punishment with the gravity of the crime committed. Some penalties may amount to retaliation against the offender rather than attempting to rehabilitate him.
- 3.** There is a lack of legislative discipline in terms of “the generality” of criminalisation in many Arab laws in a way that may allow the expansion of the provisions of the criminalisation and punishment beyond what the legislator intended.
- 4.** Senior officials should not enjoy legal protection beyond that provided for the general public and should not be immune from criticism of their actions.
- 5.** The privacy of Arab societies should not be invoked to impose restrictions on freedom of expression through the Internet and their applications beyond the legitimate limitations provided for in international conventions, in particular Article 19 of the International Covenant on Civil and Political Rights.



Recommendations

In light of the above it is recommended that:

- 1.** Any restrictions on freedom of electronic publication must comply with international standards, in particular the three-part test drawn from Article 19 of the International Covenant on Civil and Political Rights.
- 2.** The imposition of imprisonment or blocking websites on the Internet should only be used in the most serious crimes provided that the punishment is commensurate with the violation of the law.
- 3.** The imposition of high fines on violators should be avoided as it has a chilling effect on freedom of opinion and expression and leads to self-censorship among citizens, which deters them from exercising their right of expression because of fear of excessive penalties.
- 4.** Cybercrime legislation in Arab countries should be amended to conform to international standards for freedom of opinion, expression and best practices.
- 5.** Sanctions should aim at public and private deterrence and should not be a means of retaliation against the offender.
- 6.** Sanctions should not be imposed with the aim of protecting public officials and public figures in a way that exceeds the protection of ordinary citizens and undermines the public interest. Officials must tolerate criticism more than ordinary citizens.
- 7.** The use of broad, vague and ambiguous text in punitive legislation should be avoided. Definitions of offenses should be clearly understood by the general public and not only by judges and lawyers.
- 8.** It is necessary to reduce fines (payable to the State) imposed on offenders and compensate those affected in a fair manner, while fines and reparations shall not have a negative impact on the freedom of public dialogue. The compensation of employees and public figures should be symbolic, except in serious cases.
- 9.** It is necessary to look at the advantages and thus maximize the information technology revolution and address its disadvantages in a way that ensures harm reduction within the principle of proportionality between the act of wrongdoing and compensation.
- 10.** It is necessary to focus on the preventive control that precedes the occurrence of cybercrime, through activating the role of awareness-raising institutions (religious institutions such as mosques and churches, the family, education, media), by raising awareness of the seriousness of cybercrime on the family and society, especially youth, as well as awareness of the seriousness of cybercrime on perpetrators and victims.

APPENDIX



Appendix of the provisions of the laws of cybercrime in 13 Arab countries

1. Jordan: Cybercrime Law No. 27 of 2015. The original text of the law was published on page (5631) of the Official Gazette issue no. 5343 dated 1/6/2015 <http://moict.gov.jo/uploads/Policies-and-Strategies-Directorate/Legislation/Laws/Electronic-crime-Law.pdf>
2. United Arab Emirates: Cybercrime Law No. 5 of 2012 https://elaws.moj.gov.ae/UAE-MOJ_LC-Ar/00_%D8%AC%D8%B1%D8%A7%D8%A6%D9%85%20%D8%AA%D9%82%D9%86%D9%8A%D8%A9%20%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA/UAE-LC-Ar_2012-08-13_00005_Markait.html?val=AL1#Anchor11
3. Egypt: Law No. 175/2018 on Cybercrime. Published in the Official Gazette, on August 14, 2018, available at: <https://www.youm7.com/story/2018/8/19/%D9%86%D9%86%D8%B4%D8%B1-%D8%A7%D9%84%D9%86%D8%B5-%D8%A7%D9%84%D9%83%D8%A7%D9%85%D9%84-%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D9%85%D9%83%D8%A7%D9%81%D8%AD%D8%A9-%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D8%A7%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D8%A8%D8%B9%D8%AF-%D8%AA%D8%B5%D8%AF%D9%8A%D9%82-%D8%A7%D9%84%D8%B1%D8%A6%D9%8A%D8%B3/3916593>
4. Palestine: Law No. (10) of 2018 on Cybercrime https://www.lab.pna.ps/cached_uploads/download/2018/06/20/%D8%A7%D9%84%D8%B9%D8%AF%D8%AF-%D9%85%D9%85%D8%AA%D8%A7%D8%B2-16-10-%D9%85%D8%B9-%D8%B4%D8%B9%D8%A7%D8%B1-1529493779.pdf
5. Kuwait: cybercrime Law No. 63 of 2015 is available at: <https://www.e.gov.kw/sites/kgenglish/Forms/CAITLawNo.63of2015oncombatingInformationTechnologyCrimes.pdf>
6. Saudi Arabia: System of Combating cybercrime: <http://www.citc.gov.sa/ar/RulesandSystems/CITCSystem/Pages/CybercrimesAct.aspx>
7. Bahrain: Law No. 60 of 2014 on cybercrimes <http://www.acees.gov.bh/cyber-crime/anti-cyber-crime-law-in-the-kingdom-of-bahrain/>
8. Qatar: Law No. 14 of 2014 promulgating the Law on Combating Cybercrime <https://portal.moi.gov.qa/wps/wcm/connect/7a95aa55-3143-4c86-9279-6d57a1f54301/%D9%82%D8%A7%D9%86%D9%88%D9%86+%D8%A8%D8%A5%D8%B5%D8%AF%D8%A7%D8%B1+%D9%82%D8%A7%D9%86%D9%88%D9%86+%D9%85%D9%83%D8%A7%D9%81%D8%AD%D8%A9+%D8%A7%D9%84%D8%AC%D8%B1%D8%A7%D8%A6%D9%85+%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9.pdf?MOD=AJPERES>

- 9.** Sultanate of Oman: Information Technology Crimes Law No. 12 of 2011 https://www.ita.gov.om/ITAPortal_AR/MediaCenter/Document_detail.aspx?NID=64
- 10.** Syria: Legislative Decree No. 17 of 2012 on the application of the provisions of the Law of Networking and Combating Cybercrime <http://www.parliament.gov.sy/arabic/index.php?node=201&nid=4337&ref=tree&>
- 11.** Sudan: Information Crimes Act 2007 <http://www.parliament.gov.sd/ar/index.php/site/LigsualtionVeiw/273>
- 12.** Algeria: Law No. 09-04 containing special rules for the prevention and control of crimes related to information and communication technologies. Published in the Official Gazette, 16 August 2009, No. 47, p.5, https://www.arpce.dz/ar/doc/reg/loi/Loi_09-04.pdf
- 13.** Mauritania: Law No. 2016-007 on Cybercrime, published in the Official Gazette of the Republic of Mauritania on 29/2/2015 p.1354, <http://www.tic.gov.mr/IMG/pdf/loi2016007cybercrimear.pdf>

ARIJ



IN PARTNERSHIP WITH
**FRIEDRICH NAUMANN
STIFTUNG** Für die Freiheit.
Middle East and North Africa