Center for Media and Cultural Freedom

Digital Rights and Online Expression in Lebanon

A report by:
Anna Lekas Miller

THE SAMIR KASSIR FOUNDATION

This project is funded by the European Union

About the Author

Anna Lekas Miller is an independent American journalist, covering foreign and national security policies and exploring how they affect ordinary people around the world. Her reporting has been featured in *Vanity Fair*, *The Guardian*, *The Nation*, *Deutsche Welle*, *The Intercept*, *VICE* and *Rolling Stones*. She has been writing studies and conference reports for the Samir Kassir Foundation since May 2015. www.annalekasmiller.com

This report is published by the
SKeyes Center for Media and Cultural Freedom

Samir Kassir Foundation
NECG-Dib Building, 3rd floor, Sioufi Garden Street, Ashrafieh, Beirut – Lebanon
Tel: +961 1 397331 – www.skeyesmedia.org – info@skeyesmedia.org

This project is funded by the European Union
The contents of this report are the sole responsibility of the Samir Kassir Foundation
and can in no way be taken to reflect the views of the European Union.

Table of Contents

Introduction

In June 2013, the SKeyes Center for Media and Cultural Freedom partnered with the Lebanese Association for Democratic Elections (LADE) to create "Digital Rights and Election Monitoring," a research project intended to study how candidates use digital platforms to communicate with Lebanese voters, and in turn, how Lebanese voters use digital spaces to voice their political needs. However, once the elections were postponed to 2017, the project's scope evolved and eventually expanded to examine the state of digital rights in Lebanon as a whole, with an emphasis on freedom of expression on the Internet. The project particularly focused on how Lebanon's legal infrastructure impacts journalists, media-makers operating in the digital sphere, and citizens expressing themselves online, particularly through social media.

The reason for this shift in focus is two-fold. First, the media, whether traditional or social, are an essential liaison between voters and politicians. It is how citizens understand the policies of prospective candidates and analyze the information to make their decision and cast their vote. Journalists' ability to do their job – accessing politicians in power, challenging their statements, and communicating this information with the public without censorship or fear of reprisal – is an essential indicator of democracy, whether on- or offline.

Second, the definition of a journalist is changing, largely due to the Internet and the increasing popularity of 'citizen journalists' using social media and digital technology to publicize stories. This raises questions about the future of journalism in the digital age and how existing press and internet laws should adapt to the changing environment. Should a blogger have the same protections as a journalist? What about a social media user or citizen journalist posting or sharing content using a platform such as Facebook or Twitter? How should slander, libel and defamation laws affect online speech? How does current legislation impact freedom of expression online? What does digital surveillance mean for journalists, particularly those working with anonymous sources, or exposing classified or politically sensitive information? The following report addresses these questions by considering international precedents and examples where digital rights came in contact with media freedom and applying them to a Lebanese context.

The report begins by defining digital rights and providing a few examples of instances where media freedom was affected by digital rights. It goes on to describe the digital rights environment in Lebanon and how it affects its unique media ecosystem. Although there are several digital rights issues to discuss in Lebanon, this report focuses on criminalized online defamation and the practices of the Internal Security Forces' Anti-Cybercrime and Intellectual Property Rights Unit, which has been accused of both direct and indirectly censoring online journalists, bloggers and Internet users.

Overview: Digital Rights in Lebanon

Lebanon has a fragile legal framework and no legislation that specifically governs the Internet. Initially, this has had a positive effect on freedom of expression. One of the major indications of this statement is that there is no organized censorship of the media in Lebanon, the way that there is countries like Egypt and Turkey, allowing for a more open and diverse media both on- and offline.

However, the absence of laws that govern the Internet in a way that protects Internet users (including journalists and media-makers who produce their work online) means that digital rights are arbitrarily enforced. Online censorship is present and largely decided because of civilian or institutional complaints about certain content; a troubling standard for freedom of expression. Digital surveillance is present to an unknown extent and, while there are laws designed to protect personal data, there are multiple examples of evidence that they are not enforced. Currently, any data collected by the Ministry of Telecommunications via either of the major telecommunications providers, Alfa and MTC Touch, can be shared with other government entities without citizens' consent.[1]

The lack of laws governing the Internet means that, rather than being a "lawless space," the Internet is governed with pre-existing legislation, which is often outdated and never tailored to meet the digital rights needs of Internet users. The most striking example of this is the use of the Penal Code – a legal document adopted in the early 1940s[2] – to handle online defamation complaints, a practice which has been used to intimidate bloggers, raising concerns about the actual climate of freedom of expression in Lebanon.

"We do not have legislation dealing with Internet freedom, freedom of expression over the Internet or social media," Charbel Kareh said in an interview. "Instead we have the Penal Code, which dates back to 1943. Judges are applying this code to acts related to freedom of expression." Charbel Kareh is a lawyer specialized in Internet issues, who heads the Internet committee at the Beirut Bar Association.

When the Penal Code was first drafted, it was intended to maintain public order during the Ottoman Era in Lebanon. Defamation – defined as public, defamatory speech with at least two witnesses[3] – was criminalized to keep rowdy crowds from hurling insults at political figures in the public square.

[1] International, P., Exchange, S., & Progressive Communication, A. (March 2015). The Right to Privacy in Lebanon (Issue brief No. 23). Retrieved February 23, 2016, from Privacy International, Social Media Exchange and the Association for Progressive Communication website: https://www.privacyinternational.org/sites/default/files/Lebanon_UPR_23rd_session_Joint_Stakeholder_submission_0.pdf
[2] World Intellectual Property Organization. Retrieved February 23, 2016, from http://www.wipo.int/wipolex/en/details.jsp?id=6653
[3] *ibid*

Now, the same law is being applied online, where the audience of defamatory speech has been multiplied by literal millions and any post, comment or even "share" online can be deemed defamatory if the complainant is powerful enough and alerts the Internal Security Forces (ISF) of Lebanon. From here, the ISF refers the case to the Anti-Cybercrime and Intellectual Property Rights Bureau, where, at the discretion of a judge, the accused can be summoned to the Bureau for an interrogation and in some cases detained as a cybercriminal and tried in a criminal, not civil, court.

This practice is an enormous concern for both digital rights and freedom of expression advocates, and is the primary focus of this report.

What Are Digital Rights?

Digital rights are loosely defined as the right to access, use, create and share digital content free from restrictions posed by censorship, surveillance and laws silencing dissent.[4] While digital rights most immediately impact the digital or online world, digital rights have offline consequences as well. What are the consequences of our personal data being aggregated and used by companies to personalize online advertising and given to governments to form profiles of us? What happens if someone is targeted – and arrested – for what they say online?

"Digital rights are where human rights intersect with technology," Social Media Exchange (SMEX) Executive Director Jessica Dheere said in an interview. "In reality, online and offline worlds are so enmeshed that there is no decoupling; but it is still important to think about human rights in the realm of technology."

The ability of citizens to express themselves online without fear of reprisal is an essential indicator of whether or not they are living in a democracy.

How Do Digital Rights Affect Media Freedom?

As journalism and media-creation become unanimous with the Internet and social media, digital rights become intertwined with media freedom. However, digital rights protections, including but not limited to ensuring the protection of online speech, limiting mass surveillance, and regulating the collection of personal data, has not evolved so fast, leaving many legal questions up for debate.

As journalists and digital rights advocates work together to navigate the inextricable future of journalism and technology, several legal questions are raised and need to be pondered, considered, and debated with stakeholder and civilian input. Should a blogger be afforded the same legal protections as a journalist? How should slander, libel and defamation complaints be arbitrated in the online space?

Whether or not a country is safe for journalists can be measured by digital rights as well. Is a journalist or blogger or Internet user able to publish media criticizing an influential politician or politically sensitive issue without consequences? Is a journalist able to access information online? Is a journalist able to communicate freely, without fear of government or non-government surveillance?

Is a journalist able to freely publish information about any topic, without being censored? Is a journalist working in an environment where they do not need to censor themselves when reporting on certain topics?

[4] Digital Rights - IFEX. Retrieved February 23, 2016, from https://www.ifex.org/digital_rights/

In many ways, advancing and prioritizing digital rights is synonymous with advancing and prioritizing media freedom.

Blogger or Journalist?

One of the most important debates within digital rights and media freedom is whether or not a blogger should be categorized – and protected – as a journalist. While these protections vary by country, the legal result would categorize bloggers as members of the press, extending all laws pertaining to the press – such as secrecy of sources and protection from arrest and prison sentences – to bloggers, as well.

One major example of this is *Obsidian Finance Group v. Crystal Cox*, a US Supreme Court case in which Obsidian Finance Group and its partners attempted to sue investigative blogger Crystal Cox for a series of posts accusing them of money laundering and other crimes. Cox insisted that her sources remain anonymous, and Judge Andrew Hurwitz ruled that she was protected by the state of Oregon's media shield law, which protects journalists from disclosing their sources.[5]

"With the advent of the Internet, and the decline of print and broadcast media, the line between the media and others who wish to comment on political or social issues becomes far more blurred," he commented.

If Cox had not been protected as a journalist, she would have been sued for defamation, potentially costing her millions of dollars. In other countries, the unprotected nature of online media and online speech can have far more dire consequences, particularly in the face of anti-defamation, anti-cybercrime, and anti-terrorism legislation.

Social Media User or Cyber Criminal/Terrorist?

The global threat of terrorism, particularly the rise of the Islamic State's online recruitment networks, has raised many questions about where the line is drawn between freedom of expression and support for terrorism, and whether the surveillance of these social networks and censorship of this content is essential to maintaining national and international security, despite the invasion of privacy.

The threat of terrorism has also impacted legislation, some of which has an adverse impact on digital rights. Over the past three years, 13 anti-terrorism laws have been drafted in the Middle East[6] and, due to the urgency of the situation, have often been rushed through the courts, behind closed doors, leaving no opportunity for civilian input. One of the effects of this trend is one or

[5] Meyer, R. (January 21, 2014). U.S. Court: Bloggers Are Journalists. Retrieved February 23, 2016, from http://www.theatlantic.com/technology/archive/2014/01/us-court-bloggers-are-journalists/283225/

[6] Najem, Mohamed, and al-Masri, Reem. 2015. Lecture "Freedom and Privacy: the Impossible Equation," organized by the SKeyes Center for Media and Cultural Freedom in cooperation with the Global Center for Journalism and Democracy and with the support of the European Union.

multiple articles that, in an effort to stop terrorism, inadvertently affect ordinary citizens' digital rights by criminalizing certain speech or instituting mass surveillance and invasive data collection in the name of national security. In Saudi Arabia, one of these laws was used to sentence Walid Abu Kheir to fifteen years in prison[7] for a series of comments to the media and personal tweets that were accused of insulting the King.

"Certain kinds of legislation, especially anti-terrorism legislation tend to criminalize things such as expressing support for terrorism," Wafa Ben Hassine, a researcher with the Electronic Frontier Foundation said in an interview. "These laws do not provide a definition of what that means. As a result, these laws could end up being abused by law enforcement agencies to target whoever they want to target."

One recent, jarring example that affects freedom of the press is an anti-terrorism law passed in Egypt, in July 2015. The law sets a fine of approximately $25,000 for any journalist straying from government statements while publishing (in their words) "false" reports on militant attacks.

"The second effect of this type of legislation is the chilling of speech," Ben Hassine continued. "Even if a certain kind of speech is not criminalized, individuals begin to avoid speaking about certain topics just because they are afraid of being prosecuted by governmental authorities."

In addition to chilling speech, these laws normalize invasive mass surveillance measures in the name of national security or "fighting terrorism."

"There are so many laws being passed right now; we are giving up liberty for security," Reem al-Masri, a researcher for the Jordanian blog 7iber, focusing on access, surveillance and privacy in Jordan and throughout the Middle East remarked at a panel on Freedom and Privacy[8] hosted by the SKeyes Center for Media and Cultural Freedom in May 2015.

"How does the monitoring of communication and social media networks happen?" she continued. "Highly sophisticated technologies are going into the private lives of people."

[7] Saudi Arabia: Prominent Activist Marks Year Behind Bars. (April 15, 2015). Retrieved February 23, 2016, from https://www.hrw.org/news/2015/04/15/saudi-arabia-prominent-activist-marks-year-behind-bars

[8] Najem, Mohamed, and al-Masri, Reem. 2015. Lecture "Freedom and Privacy: the Impossible Equation," organized by the SKeyes Center for Media and Cultural Freedom in cooperation with the Global Center for Journalism and Democracy and with the support of the European Union.

What is the State of Digital Rights in Lebanon?

Traditionally, Lebanon has a reputation as having one of the freest and most democratic media environments in the Arab World. Freedom of expression is enshrined in Article 13 of the Lebanese Constitution, reading: "The freedom to express one's opinion, orally or in writing, the freedom of the press, the freedom of assembly, and the freedom of association shall be guaranteed *within limits established by the law*." [Italics added by author]

However, while the Lebanese media presents a diversity of perspectives, many of its critics credit this to the relationship of the media with the sectarian structure of the government rather than to genuine media plurality. Though, unlike many of its neighbors such as Egypt and Syria, Lebanon does not have a dictatorship-like leader in power controlling the media. The media nevertheless reflects each sect and their political priorities.

Secondly, the phrase "*within limits established by the law"* needs to be investigated and interrogated. What are these limits and do they constrict freedom of expression online?

The short answer is, yes.

Lebanon, Social Media and Digital Rights

Although television is perceived as the "most credible" news source according to Lebanese media consumers,[9] blogs have an important – and unique – role in the Lebanese media ecosystem. As independent, politically unaffiliated news sources, blogs represent an increasingly important alternative to the traditional, sectarian media.

However, though there is a legal infrastructure to protect freedom of expression in the press, this protection does not extend to media produced online, leaving digitally-produced journalism, particularly blogs, in a legal gray area. On the one hand, this keeps the Internet free of regulations on content – a battle that has been fought once in 2010,[10] when civil society stopped the a parliamentary vote on a controversial e-transactions law that would have passed articles legalizing warrantless search and seizure of electronic files, hard drives and computers, and again in 2012 when several of the same activists halted the so-called Lebanese Internet Regulation Act,[11] which would have instituted government control of online publications.

[9] Youth and Media in Lebanon: 96% use their mobile phones while the television remains the "most credible" source | United Nations Educational, Scientific and Cultural Organization. (May 28, 2015). Retrieved February 23, 2016, from http://www.unesco.org/new/en/beirut/single-view/news/youth_and_media_in_lebanon96_use_their_mobile_phones_while_the_television_remains_the_most_credible_source/#.VsxAIJN95o4
[10] Stop the New Internet Law in Lebanon. (June 10, 2010). Retrieved February 23, 2016, from http://www.smex.org/stop-the-new-internet-law-in-lebanon/
[11] York, J. C. (April 2, 2012). Proposed Laws in Lebanon and Iraq Threaten Online Speech. Retrieved February 23, 2016, from https://www.eff.org/deeplinks/2012/03/proposed-laws-lebanon-iraq-threaten-online-speech

Unfortunately, the lack of legislation or regulation also has an adverse effect. First, the Internet is not entirely free of censorship, which, due to a lack of regulations or protections, is enforced in an arbitrary and unpredictable way. One example of this is blocking websites. There are no legal parameters for blocking websites, meaning that the online sphere is neither a protected space for free expression, nor an example of the highly regulated, formalized censorship indicative of several dictatorships. Instead, websites are blocked by Internet users calling in complaints to the Anti-Cybercrime and Intellectual Property Rights Bureau, who then refers it to the Ministry of Telecommunications, who blocks the website; meaning that civilians, private companies and government institutions have the ability to request Internet filtration.

According to statistics from the Lebanese NGO Social Media Exchange (SMEX),[12] there are currently 50 websites blocked in Lebanon, which mostly fall into the categories of escort services, gambling, underage pornography, or Israeli websites. However, not all websites falling into these categories are blocked, pointing to the arbitrary nature of the practice.

Second, in the absence of legislation tailored to the Internet, pre-existing laws – such as the anti-defamation articles in the Penal Code, as previously mentioned – are used to arbitrate complaints relating to online content, particularly against bloggers who are accused of insulting a powerful political figure or corporation. While Lebanon does not have explicit, stand-alone anti-cybercrime or anti-terrorism laws, the anti-defamation articles fulfill a similar purpose of both directly targeting activists and dissidents and, by using these cases to set an example, intimidating online journalists, bloggers and Internet users from speaking about certain subjects, thus paving the way for self-censorship and the chilling of speech.

[12] Mapping blocked websites in Lebanon 2015. (March 26, 2015). Retrieved February 23, 2016, from http://www.smex.org/mapping-blocked-websites-in-lebanon-2015/

A Closer Look at the Anti-Cyber Crime and Intellectual Property Rights Bureau

In 2006, the Internal Security Forces established the Anti-Cybercrime and Intellectual Property Rights Bureau [herein: Cybercrime Bureau] to strengthen cyber-security and combat cybercrimes in Lebanon.

However, while the Cybercrime Bureau is designed to address online crimes such as identity theft, money laundering and child pornography, by merit of being the only unit within the ISF specialized to Internet-related crimes, it also handles online defamation, libel and slander complaints. This means that it has given itself the authority to summon, detain and interrogate online journalists, bloggers and Internet users accused of defamatory online speech, and, by nature of the Bureau, treat them as suspected cybercriminals. It is worth mentioning that his report is not addressing the debate questioning the legality of the process that led to the very establishment of the Bureau.

Summoning of Journalists

According to statistics from SMEX, there have been 18 summonses to the Cybercrime Bureau since this practice began in 2010. While in most cases the worst punishment is a fine, there are many troubling aspects of the procedure, which point towards a lack of regard for freedom of expression.

First, citizens are often summoned under vague – or in certain instances, false – premises. Lebanese blogger Gino Raidy documented his experience on his blog (reprinted on NOW Media),[13] reporting that he received a phone call from an unknown number and was requested to present himself after publishing a blog post reviewing a social networking service. Nineteen year old Karim Hawa was told that he had purchased a stolen smart phone and asked to report to the Bureau. He was then held for four days, interrogated and unable to recover his laptop and phone – which had been requested – for another two months.

Second is the issue of data collection and the lack of regulations for data protection; a concern illustrated by the seizure of Hawa's laptop and mobile phone. In many ways, this is a systemic issue. In 2014, an iPhone and Android application was released that allowed users to access personal data, such as address, phone number, and marital status, by searching for their license plate number,[14] raising the question of whether or not the telecommunication companies, Alfa and MTC Touch, were protecting user data or not. While the app is no longer available for download, it illustrates the distinct possibility that the Ministry of Telecommunications could share

[13] Raidy, G. (January 30, 2014). The Details of What Happened With Me at the Cybercrime Bureau. Retrieved February 23, 2016, from https://now.mmedia.me/lb/en/blogs/533182-the-details-of-what-happened-with-me-at-the-cybercrime-bureau
[14] Najem, M. (May 15, 2014). In Lebanon, Apps Let You Get Someone Else's Personal Info With Ease. Retrieved February 23, 2016, from http://www.slate.com/blogs/future_tense/2014/05/15/in_lebanon_apps_let_you_get_someone_else_s_personal_info_with_ease.html

information with other ministries and government departments (including the Internal Security Forces), without checks, balances or regulations on Lebanese citizens' personal data. Worst, there are no guarantees that individuals within the Ministry of Telecommunications or the telecom companies cannot disclose private information to non-state actors, whether private companies or political parties.

Lastly, is the issue of censorship. Often, those who have been summoned to the Cybercrime Bureau are instructed to sign a document, stating that they will not write defamatory or slanderous content about the accuser again; a policy that has been described as direct censorship by the Bureau and paving the way for self-censorship, as well.

"The procedure is used to intimidate people," Executive Director of MARCH Lebanon, Lea Baroudi said in an interview. "This does not only provoke censorship by the Bureau; it provokes self-censorship as well."

While there have been fewer summonses of bloggers and Internet users to the Cybercrime Bureau since the end of 2013, the decline is suspected to be the result of self-censorship, rather than the Cybercrime Bureau changing its policies. MARCH Lebanon has recently created a legal hotline (+961 70 235463), designed to offer free legal support for those called into the Cybercrime Bureau to know their rights and resist any charges. However, there is still no solution to the systemic problem of the legal system, which puts these complaints under the purview of the Cybercrime Bureau in the first place.

Lack of Transparency

In addition to online journalists, bloggers and Internet users being summoned under unclear – or outright false – pretenses, very little is known about the Cybercrime Bureau itself. There is no website. Its address, phone number and other contact information are not openly accessible to the public. Head of the Cybercrime and Intellectual Property Rights Bureau, Major Suzanne Hajj Hobeiche rarely gives interviews to journalists and did not respond to the SKeyes Center's multiple requests for comment.

As a result, the majority of the information pertaining to the Cybercrime Bureau has been attained through leaks and hacks, such as the July 2015 Hacking Team data hacks,[15] and is not readily transparent, nor otherwise available to the public.

[15] York, J. (August 3, 2015). Hacking Team Leaks Confirm What Arab Privacy Advocates Already Knew. Retrieved February 23, 2016, from https://www.eff.org/deeplinks/2015/08/hacking-team-leaks-confirm-what-arab-privacy-advocates-already-knew

Instrument of Surveillance

While the extent of digital surveillance in Lebanon is still unknown, there are multiple pieces of evidence that the Cybercrime Bureau is at least partially responsible for implementing both online and mobile surveillance in Lebanon. In July 2015, the Hacking Team data leak revealed a series of e-mails confirming that the Cybercrime Bureau had used FinFisher[16] technology, a spyware technology that exploits security flaws in order to monitor users, to access the mobile game "Angry Birds" allowing it to track users' activity and communications through the iPhone and Android application.

What is the Bureau's Response?

Major Suzanne Hajj Hobeiche has voiced her concern for the Cybercrime Bureau's actions against journalists on multiple occasions, placing the blame on the legal system that puts online defamation complaints under the jurisdiction of the Cybercrime Bureau. However, while she has emphasized that the bureau does not monitor social networking sites, nor summon people in for expressing their opinion, this practice remains ongoing.

[16] Marczak, B., Senft, A., Poetranto, I., & McKune, S. (October 15, 2015). Mapping FinFisher's Continuing Proliferation. Retrieved February 23, 2016, from https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

Conclusion and Suggestions

As Lebanon embraces the digital world and its new media expand and evolve to bypass the constrictions of traditional media, it is important that a digital rights infrastructure is in place to protect freedom of online expression for both digital journalists and citizens. First, it is important to state that entities such as the Anti-Cybercrime and Intellectual Property Rights Bureau and practices such as necessary and proportionate surveillance are necessary and essential to national security. In our criticism, we do not propose the dissolution of neither this Bureau nor these practices, but instead amendments to make them more conducive to the freedom of online security and digital rights at large. However, the legal system that implicates online journalists and Internet users accused of defamation, libel and slander as cybercriminals needs to be amended, for both the modernization of media freedom and the larger issue of freedom of expression within a democracy. There are several legal approaches that could work towards making this a reality.

1. Update the current Press Law to protect freedom of expression for online journalists and bloggers, giving online media-makers the protection to create critical, sarcastic or controversial content without fear of consequence.
2. Remove "libel, slander and defamation" from the Penal Code, making it a civil, rather than a criminal offense, thus removing it from the jurisdiction of the Anti-Cybercrime and Intellectual Property Rights Bureau.
3. In addition to decriminalizing online defamation to allow for freedom of expression, it is essential that Lebanon's surveillance of citizens is necessary and proportionate. Data collected by Telecommunications companies such as Alfa and MTC Touch should be kept private, only accessible through a warranted search.
4. Respect and enforce Lebanese Law No. 140, which mandates the right to secrecy of all wired and wireless communications, and Article 17 of the International Covenant on Civil and Political Rights (to which Lebanon is a signatory), which reinforces Article 12 of the Universal Declaration of Human Rights (UDHR), providing that "no one should be subjected to the arbitrary or unlawful interference with his privacy, family, home, or correspondence, nor to unlawful attacks on his honor or reputation.