Device Seizures in Lebanon

Assessing the Legal Framework concerning device seizures in Lebanon

January 2021

smex.org

ACKNOWLEDGEMENTS

Marianne Rahme, SMEX's legal advisor was the researcher and author of this report.

The report was edited by **Grant Baker,** who served as a contributing author, **Nourhane Kazak** provided copyediting support. **The Language Platform** translated this report into Arabic.

The research was generously funded by **Heinrich Böll Foundation (Heinrich-Böll-Stiftung)**

All errors and omissions are the responsibility of SMEX.

SMEX is a Lebanese NGO that since 2008 has worked to defend digital rights, promote open culture and local content, and encourage critical, self-regulated engagement with digital technologies, media, and networks across the Middle East and North Africa (MENA).

www.sme**x.org**

A January 2021 Publication by SMEX

Kmeir Building, 4th Floor, Badaro, Beirut, Lebanon

Table of Content

Executive Summary

We have witnessed in the last couple of years a striking increase in the number of devices seized by security agencies in Lebanon, a phenomenon that became more pronounced following the October 2019 uprising. When it comes to these seizures, the legal framework is vague and often exploited or circumvented since it is subject to many unlawful practices by the authorities.

Lebanon has signed numerous international treaties with privacy implications. Moreover, the Lebanese constitution protects the right to privacy, albeit not explicitly. However, the right to privacy was guaranteed by the Constitutional Council in a decision that dates back to 1999.

At the national level, the criminal procedure code, modified in 2001, enables the examining magistrate to order device seizures. Law 140[1], adopted by the Cabinet in 2009[2], adds another administrative authorization, permitting certain branches of the executive branch to order these seizures. This law also adds conditions to be respected: the decision needs to be taken in cases of extreme urgency and needs to be written and justified. The E-transactions Law, passed in 2018, transfers the authority to search and seize devices in investigations from the examining magistrate to the public prosecution without any "limitations."

During the October Uprising, security agencies arrested protesters and frequently seized their devices, which constitutes a breach of privacy and an infringement on basic rights. In response to these seizures, a circular was issued by the General Prosecutor on December 3, 2019. The circular emphasizes the detainees' basic rights and reminds of the "constitutionality" of the right to privacy especially when it comes to devices, however, it does not effectively rein in the search and seizure of devices.

1 Law 140/1999, Available at: http://www.legallaw.ul.edu.lb/Law.aspx?lawId=198664

2 Privacy International & SMEX (2019, January), *State of Privacy in Lebanon*. Available at: https://privacyinternational.org/state-privacy/1081/state-privacy-lebanon

Introduction

In Lebanon, we have witnessed an increase in the crackdown on online freedom of expression since the 2015 protests where protesters who are detained often have their mobile phones seized and searched. During the October 2019 protests, the security agencies also searched the mobile phones of detained protestors, often without a warrant, committing a violation of people's right to privacy.

Nowadays, mobile phones are an integral part of our day-to-day interaction with the world, be it work or our personal lives. They are also a critical tool for activists and human rights defenders trying to communicate with one another and organize. Our mobile phones contain a plethora of personally identifiable information, including our location, our passwords, our social media accounts, private chats, pictures, and more. If our phones are searched against our will, it constitutes a violation of our right to privacy, which has been guaranteed by the Constitutional Council.[3] However, the judiciary and security agencies regularly disregard and violate this right, hiding behind vague articles in the legal framework.

We are trying to answer the question: how does Lebanon's legal framework address the search and seizure of these devices? Despite the existence of a legal framework regulating the surveillance of communications and the confiscation of devices, the judiciary, and the security agencies tend to circumvent and exploit this framework, leading to violations of privacy rights. The Cybercrime and Intellectual Property Rights Bureau, an agency under the mandate of the Internal Security Forces (ISF), is often responsible for detaining activists and searching their devices. In Lebanon, the legal framework for surveillance and data protection remains archaic, and citizens' rights remain the least of the state's concerns.

Threats to civic space in Lebanon have increased dramatically in the past four years, with a growing number of detentions related to freedom of expression since 2016. Economically, the country is also facing a major crisis, with rising inflation rates and extreme poverty. Additionally, corrupt sectarian warlords still maintain control over the state's institutions.[4]

Throughout the October uprising, which began on October 17, 2019, different branches of the ISF and the Lebanese Armed Forces (LAF) proceeded with unjustified brutality against the protesters as well as arbitrary arrests of protesters and unlawful device searches. These seizures and searches reached a peak on January 14, 2020. Since the protests started in late 2019, security services have searched devices of protesters to collect and analyze data from their phones that can be used as evidence against them, leading to more arrests. Many of the arrested protesters said no search warrant or written judicial decision was presented to them, giving the ISF authorization to search the phones.[5]

Most recently, the government declared the state of emergency[6] alongside a state of general mobilization in response to the global pandemic and the Beirut explosion, which occurred on August 4, 2020, restricting the freedoms and liberties of the people. Ever since the declared states of emergencies, there have been continued restrictions on freedom of expression and privacy rights. We have witnessed a large number of cases, arrests, and summons related to social media posts, online activism, and whistleblowing. In many of these cases, security agencies often operate outside of the law during the investigation.

These seizures have a negative impact on freedom of speech, privacy rights, and the right to assemble and protest. People were arrested based on location tracking, pictures, or chats on their devices, and were convicted of acts of sabotage.[7]

Nazek Khatib[8], a public prosecutor (مدعي عام), told us there is no actual, solid, legal framework for the access to devices (الولوج). Therefore, when someone is called in for questioning, the ISF does not have a strong body of legal requirements to abide by.

3 Constitutional Council, Lebanon, decision number 2/99, 24/11/1999.

4 محمد زبيب، 2019/10/29،الأزمة الاقتصادية في لبنان: ما هي؟ ما العمل؟، الاخبار، متوفر على :
https://al-akhbar.com/Video/278043/ما-هي-في-لبنان-الأزمة-الاقتصادية

5 غيدة فرنجية، نور حيدر، سارة ونسا، 16-10-2020، كيف استخدمت السّلطة سلاح التوقيفات لقمع حرّية التظاهر والاعتراض؟، العدد 66 من مجلة المفكرة القانونية – لبنان
"الثورة في مواجهة السّلطة وعنفها"، المفكرة القانونية، متوفر على: https://legal-agenda.com/كيف-استخدمت-السّلطة-سلاح-التوقيفات-لق/

6 The State of Emergency was to end on August 18th 2020 because the subsequent renewals are considered illegal. The renewal ended on September 18th but some of the army's prerogatives were renewed until December 31st.

7 غيدة فرنجية، نور حيدر، سارة ونسا، 16-10-2020، كيف استخدمت السّلطة سلاح التوقيفات لقمع حرّية التظاهر والاعتراض؟، العدد 66 من مجلة المفكرة القانونية – لبنان
"الثورة في مواجهة السّلطة وعنفها"، المفكرة القانونية، متوفر على: https://legal-agenda.com/كيف-استخدمت-السّلطة-سلاح-التوقيفات-لق/

8 Interview with Ms. Nazek Khatib, public prosecutor.

In this report, we will discuss the legal framework for device seizures in Lebanon and its impact on human rights in general. The search and seizure of mobile phones and other devices are regulated by the Constitution, the Criminal Procedure Code, Law No. 140 on Surveillance, and the E-Transactions Law. In addition to the legislation concerning device seizures, we will also shed light on jurisprudence around the search and seizure of mobile phones, as well as the methods security agencies have used for searching devices in the past year.

Methodology

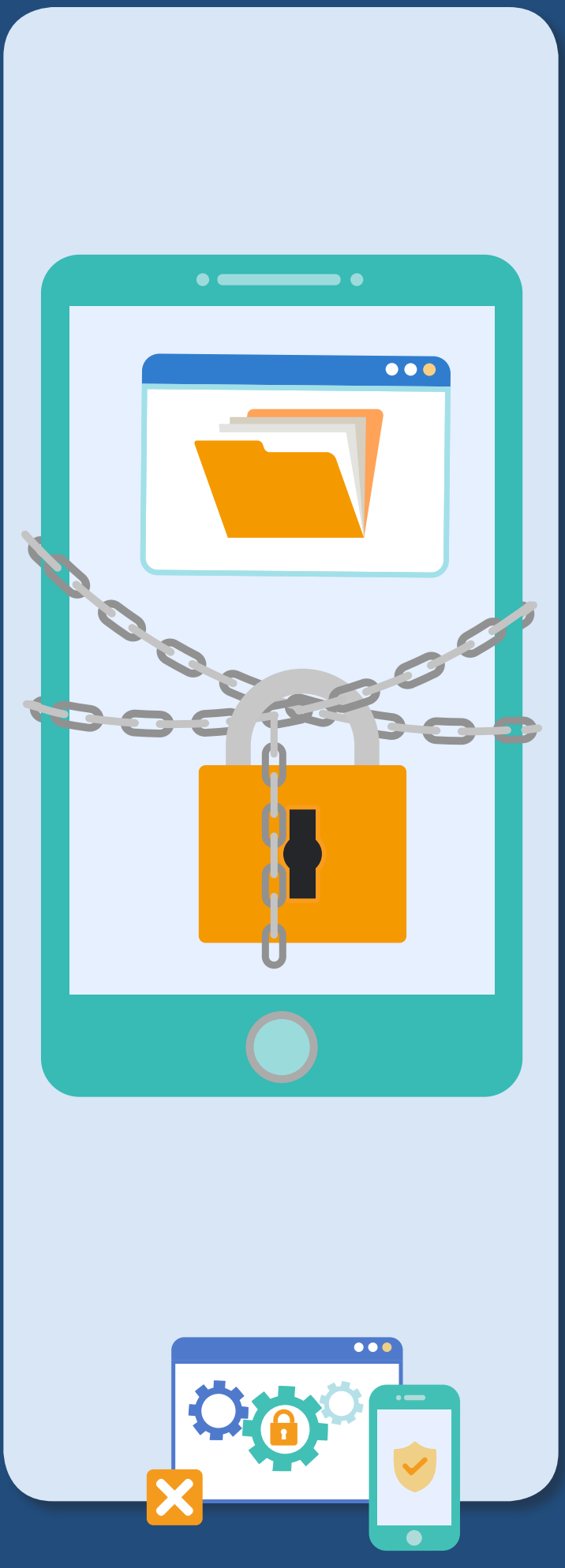
The research for this report consists of desk research and stakeholder interviews carried out between November 2020 and January 2021.

First, we conducted a literature review based on the previous research from the Legal Agenda, SMEX, and other organizations, as well as media outlets, to map the Lebanese legal framework for device seizures. Previously, SMEX has explored the legal framework for privacy, generally, as well as surveillance.

We then prepared a questionnaire for key stakeholders from the public, private, and humanitarian sectors that we identified from our initial research. We invited them to participate in interviews to help with our research. Ultimately, we spoke with lawyers, researchers, judges, and public prosecutors.

Interviewees include Nazek Khatib, a public prosecutor and the Attorney General of Appeal in Mount Lebanon, who has experience in handling cases involving device seizures. We also interviewed Rabih Maalouf, a judge in the Misdemeanors Court of Appeals in Beirut, who wrote the first concurring opinion concerning device seizures and the protection of privacy in Lebanese jurisprudence.

We spoke with Ghida Frangieh, a Lawyer at the Legal Agenda who has worked on device seizures as a defendant for privacy rights and defense rights. She also managed cases of arrested protesters from the October uprising. Additionally, we interviewed Charbel Kareh, a lawyer specialized in information technology and property rights, and the previous President of the Information and Communication Technology Committee of the Beirut Bar Association. He is also a member of the Lebanese Parliament's Information and Communication Technology Committee (ICT). Finally, we spoke to Diala Chehade, another lawyer specialized in International Criminal Law, who has worked on a case concerning device seizures in the October uprising period.



The Legal Framework: Device Seizures in Lebanon

The right to privacy is not explicitly protected in the Lebanese Constitution, the place of residence is deemed inviolable in Article 14 of the Constitution, which has been interpreted as implicit protection of privacy. Article 14 states: «The citizen's place of residence is inviolable. No one may enter it except in the circumstances and manners prescribed by law». When it comes to individual liberty and freedom of expression, Articles 8 and 13 indirectly guarantee those rights. Legal experts have interpreted that these articles can protect the secrecy of all means of communications, yet this protection is not stated explicitly.[9]

Concerning the legal framework, we will discuss international treaties and national laws. We will assess the Criminal Procedure Code, Law 140/1999 on the secrecy of communications, E-transactions Law 81/2018 all of which apply to the search and seizure of mobile phones and other devices. We will also analyze one of the only cases discussing device seizures: the 2018 concurring opinion by Judge Rabih Maalouf.

The Criminal Procedure Code in 2001 gives the examining magistrate the authority to search devices. Law 140 adds conditions to searches and seizures but also introduces the concept of "administrative" authorization, which allows the ministry of interior and ministry of defense to authorize surveillance and searches directly. Most recently, the E-transactions law alters the concept of "judicial authorization" giving both the examining magistrate and the public prosecutor the authority to order the search and seizure of devices.

1. International Treaties

The right to privacy is a fundamental human right and is consecrated in several treaties, it enforces other rights such as freedom of expression and constitutes a basis for democratic societies.

The right to privacy embodies the principle that individuals should have an area of autonomous development, interaction, and liberty, a "private sphere" with or without interaction with others, free from arbitrary State intervention and from excessive unsolicited intervention by other uninvited individuals.[10]

Lebanon has signed numerous treaties with privacy implications, including the Universal Declaration of Human Rights; the International Covenant on Civil and Political Rights; the International Convention on the Elimination of All Forms of Racial Discrimination (except for Article 22); the Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment; the Convention on the Rights of the Child; the International Covenant on Economic, Social and Cultural Rights; the International Convention for the Protection of All Persons from Enforced Disappearance; the Convention on the Rights of Persons with Disabilities; the United Nations Convention against Transnational Organized Crime; the Cairo Declaration on Human Rights in Islam; and the Arab Charter on Human Rights.[11]

As a signatory to these treaties, Lebanon is bound to respect that: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation" (Article 12 UDHR, reinforced by Art 17 ICCPR).[12]

2. Criminal Procedure Code

The Criminal Procedure Code, in its 2001 modification, regulates the regime applicable to search and seizures, and gives the examining magistrate, also referred to as the investigative judge[13], the power to order the search and seizure of phones and other devices. Below is the original excerpt of the Code:

9 Privacy International & SMEX (2018, January), *State of Privacy Lebanon.* Available at: https://smex.org/wp-content/uploads/2018/02/State_of_Privacy_01_18.pdf

10 Martin Scheinin, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 2009, A/HRC/17/34.

11 Privacy International & SMEX (2018, January), *State of Privacy Lebanon.* Available at: https://smex.org/wp-content/uploads/2018/02/State_of_Privacy_01_18.pdf

12 Privacy International & SMEX & APC (2015, March), *Universal Periodic Review, Stakeholder Report: 23rd session, Lebanon. The Right to Privacy in Lebanon.* Available at: https://privacyinternational.org/sites/default/files/2018-02/Lebanon_UPR_23rd_session_Joint_Stakeholder_submission_0.pdf

13 A judge before whom crimes requiring an expansion of investigations are referred in order to identify who has committed them, clarify their circumstances and gather evidence. The role of the investigative judge or the examining magistrate is defined in the Lebanese Criminal Procedure Code in Part III - Investigative judges and their duties. The submission containing the Public Prosecutor's Office's charges is filed with the First Investigating Judge. Actions brought directly by victims of crimes discovered during their commission or immediately afterwards based on their personal charges are also submitted to him. For more: http://legallaw.ul.edu.lb/LawArticles.aspx?LawTreeSectionID=260055&lawId=244483&language=ar

Article 98 (date of entry into force: 02/08/2001):[14]

> "The examining magistrate may visit the crime scene personally with the court clerk to inspect it or to search a suspected house for incriminating materials or items that may be of use to the investigation. The examining magistrate must notify the Public Prosecutor of their visit.
>
> If the Public Prosecutor accompanies the examining magistrate, the latter shall carry out the search and inspection in the former's presence. If not, the examining magistrate may carry out these procedures by themselves. The inspection or search must take place in the presence of the personal plaintiff and the defendant.
>
> In the event that the plaintiff or defendant refuses or fails to appear, the inspection or search process shall be carried out either in the presence of their attorney, two witnesses from among their family members or two witnesses appointed by the examining magistrate [...]
>
> If confidential documents are seized during the search process, they shall be numbered, and only the examining magistrate and their owner shall be allowed to view them.
>
> Such documents shall be kept in sealed envelopes upon which a statement is affixed indicating their number, references and confidential nature."

Article 98 stipulates that the examining magistrate in a case where they has to proceed with the search of a house/crime scene, has to notify the public prosecutor of the search. The public prosecutor can decide to go with the examining magistrate but his presence is not mandatory.

The most important part of this article, however, establishes that: when it comes to searching confidential documents, only the examining magistrate has the authority to see them. This article regulates searches and seizures and gives authority to the examining magistrate.

While Article 98 addresses search and seizure generally, Article 103 pertains to the search and seizure of devices. Ghida Frangieh[15], Lawyer at the Legal Agenda argues that Article 103 of the Criminal Procedure Code has serious implications on device seizures:

Article 103 (date of entry into force: 02/08/2001):[16]

> "If the examining magistrate believes that keeping all or some of the seized items does not benefit the investigation, they shall return them to their owner, provided that there is no legal dispute regarding the ownership of the said items.
>
> If there is a serious legal dispute regarding the ownership or possession rights of the seized item to be returned, the examining magistrate shall delay the return process until the dispute is resolved.
>
> In the event that the personal plaintiff or defendant request the retrieval of a seized item, the examining magistrate shall decide on their request after consulting with the opposing litigant and the Public Prosecution.
>
> The magistrate's decision in this regard may be appealed within a period of twenty-four hours after the affected litigant is notified."

According to Ms. Frangieh, the article implies that "If the device is deemed to contain evidence necessary for the investigation, the information on it can be downloaded/written in the report and the device returned to the defendant. And if the examining magistrate decides that the device is not useful for the investigation (no relevant evidence) he returns it to the defendant.

In summary, the Criminal Procedure Code gives the authority to the examining magistrate to seize and search devices.

The examining magistrate determines what data is necessary and related to the case itself. The examining magistrate gets to seize this data. The data should not be disclosed without prior consent from the accused. Although Article 103 applies in most cases, there are other articles that regulate drug-related cases.

3. Law 140/1999: Telecommunication Interception Act

The Telecommunication Interception Act of December 27, 1999 (later on referenced as Law 140[17]), which the cabinet adopted in 2009, is the first law directly regulating the interception of communications. Law 140 outlines additional conditions for the seizure of devices, and it also

14 Article 98 of the Lebanese Criminal Procedure Code, Available at: http://legallaw.ul.edu.lb/LawArticles.aspx?LawArticleID=979538&LawId=244483&language=ar

15 Interview with Ms. Ghida Frangieh, Lawyer at the Legal Agenda

16 Law 140/1999, Available at: http://www.legallaw.ul.edu.lb/Law.aspx?lawId=198664

17 Law 140/1999, Available at: http://www.legallaw.ul.edu.lb/Law.aspx?lawId=198664

establishes the concept of "administrative authorization." This allows the executive branch to order the search and seizure of devices under certain conditions.

Law 140 stipulates the right to the secrecy of one's communications, including internal, external, wired, and wireless communications. While the law guarantees the protection of these communications, it permits wiretapping, surveillance, and interception in cases of **extreme urgency.** In these cases, either a judicial authority or an administrative authority must provide authorization.

Article 2

> "In cases of extreme urgency, the first examining magistrate in each governorate may decide, either by themselves or upon a written request by the judge entrusted with the investigation, to intercept communications carried out through any of the means mentioned in Article 1 of the present Law when prosecuting a crime that is punishable by deprivation of liberty for a minimum of one year. The magistrate's decision shall be made in writing and shall be justified and not subject to any form of appeal."

Article 3

> "The examining magistrate shall indicate in their decision the means of communication to be intercepted, the crime being prosecuted or investigated and the duration of interception, provided that the latter does not exceed two months. This interception period shall be renewable strictly within the same rules and conditions."

In Article 2 and Article 3, the Law states that intercepting one's data can be authorized by court order in case of emergency if the victim is a suspect in a crime. The authorization (the court order) should mention the means of communication, the subject matter of the procedure, the subject matter of the prosecution or the investigation, and the duration of interception, which may not exceed two months.[18] In the case of judicial authorization, the law only mentions the examining magistrate, however, it does not explicitly exclude the public prosecutor or other judicial figures from ordering a search or seizure of a device.

Article 9

> "The Minister of Defense and the Minister of Interior may authorize the interception of communications by virtue of a written and justified decision, upon the approval of the Prime Minister, if the purpose is to collect information intended to fight terrorism, crimes against state security and organized crime. The decision shall indicate the means of communication to be intercepted, the information to be collected and the duration of interception, which shall be renewable strictly within the same rules and conditions."

According to Article 9, Administrative authorization can be given by either the Minister of Interior or the Minister of Defense after getting approval from the Prime Minister to fight terrorism, crimes against state security, and organized crime, none of which are clearly defined in the law. This decision must be **written, justified, and approved by the Prime Minister**, and should specify the means of communication, the subject matter of the procedure, the subject matter of the prosecution or the investigation, and the duration of interception, which may not exceed two months.[19] This set of articles allows the executive to overstep the judiciary: by giving this power to the Administration, the law potentially facilitates breaches of privacy motivated by political interest since the Ministries can decide to intercept communications without any oversight from the judiciary. The "administrative authorization" could lead to cases of mass surveillance.

On the other hand, the law sets conditions that must be respected for the surveillance to be lawful. The problem with the conditions is that the decision cannot be contested or opposed by the victim, so they are not guaranteed. Nothing can guarantee the conditions will be met if the victim cannot oppose the decision and ask for it to be revised.

4. Law 81/2018: The E-transactions Law

The E-transactions Law transferred the authority to seize/search devices in the investigations from the examining magistrate, in case of extreme necessity, to the public prosecution, without any real limitations. This law does not adequately limit the ability for judges to order searches and seizures, which is a regression in the protection of the constitutional right to privacy.[20]

18 Privacy International & SMEX (2018, January), *State of Privacy Lebanon.* Available at: https://smex.org/wp-content/uploads/2018/02/State_of_Privacy_01_18.pdf

19 Law 140/1999, Available at: http://www.legallaw.ul.edu.lb/Law.aspx?lawId=198664

20 غيدة فرنجية، 2020/10/01، معارك المادة 47: كيف انتزعت الانتفاضة حقوق الدّفاع للمحتجزين؟، العدد 66 من مجلة المفكرة القانونية – لبنان، متوفر على: https://legal-agenda.com/معارك-المادة-47-كيف-انتزعت-الانتفاضة-حق/#_ftnref12

Law no. 81 of 2018 on E-Transactions and Personal Data (E-Transactions Law) further facilitates device seizures and offers less protection than Law 140, giving the prosecutor the right to approve the seizure of devices, as opposed to just the examining magistrate. In September 2018, the Lebanese parliament passed the E-Transactions Law.[21] This Law regulates the protection of personal data in theory, but in practice it remains weak. Initially introduced in 2004, as a law that focused exclusively on electronic transactions, it does not reflect the current digital reality or provide effective protection of personal data. The articles are largely vague, lacking important definitions of key terms, such as consent, regulation, and enforcement for the conduct of data processing officers.

According to the law, public entities do not have to go through the same process as private entities to process data (Article 94). Prosecutors also have almost unrestrained authorization to access, process, and store personal data as long as prosecutors respect required procedures (separate and detailed report... see Article 123).

Article 123 of this law stipulates:

> "For every IT/digital evidence seized, a record shall be written detailing the seizure, retention, analysis, examination or transfer thereof from one authority to another, etc. The record shall also include a detailed overview of all procedures, actions, and authorities that held the evidence and method of transferring the same, particularly those ensuring evidence integrity from the moment of seizure thereof.
>
> In all cases, a true copy of the as-is digital evidence (data and software) shall be maintained, and the electronic medium used to store the same shall be stamped, sealed, and submitted to the relevant judicial authority along with the written record.
>
> Without prejudice to the provisions of this Chapter, in case of seizure of any IT evidence/ data stored on a portable electronic medium such as a CD or a laptop, the provisions of the Criminal Procedure Code shall be applied in relation to searching and impounding evidence in flagrant and non-flagrant offenses, particularly Articles (33) and (41) thereof."

Ghida Frangieh, lawyer at the Legal Agenda, tells us:

> "According to the Code of Criminal Procedures and to the E-transactions Law, especially in its Article 123, devices may only be seized (ضبط) by order of the prosecutor (or later by order of the investigating judge) if the device was used in the commission of the crime if it contains evidence that helps to uncover the truth or is useful to the investigation. The confidentiality of information that is not related to the subject of the investigation and the privacy of people of good faith or not of concern should be respected."

Currently, the search of devices is subject to the rules related to the search of objects. However, it should be subject to rules related to the search of private communications.

Article 124 also sets regulations concerning the seizure of digital evidence, starting "Any data or digital evidence stored in an IT system located in the Lebanese territories may be seized..." Charbel Kareh, a lawyer who specializes in data protection, tells us that[22] "if access thereto is possible from the IT system falling with the search warrant scope, any data stored in an IT system may be accessed and seized, whether they are in Lebanon or abroad. "

Article 121 also states that **data not related to the criminal case should be protected.** Unfortunately, the application of this law is quite different since most prosecutors tend to consider all data as evidence, and courts do not often distinguish between the nature of the data and the means of collecting it. Moreover, Article 122 of the Law adds the **condition of "non-alteration"** of the seized data. "The court may estimate, at its own discretion, the power of proof and authenticity of the digital/IT evidence, provided that such evidence is not altered in any way during seizure, retention, or analysis."

The E-transactions law remains weak when it comes to privacy protection. It transfers the authority to access devices to the public prosecutor, a party in litigation.

Charbel Kareh tells us the problem concerns the penal investigations procedure in the country and the fight should continue to change the legislation. While passwords and other methods to prevent access to mobile phones may reduce the chance

21 SMEX, Law No. 81 Relating to Electronic Transactions and Personal Data, Available at: https://smex.org/wp-content/uploads/2018/10/E-transaction-law-Lebanon-Official-Gazette-English.pdf

22 Interview with M. Charbel Kareh, lawyer specialized in data protection.

that the authorities can access someone's device, the prosecutor can decide to decrypt the device without any legal consequence. Therefore we need to amend the legislation to offer better protections for privacy because relying solely on password strength and other digital security techniques will not adequately protect those who are detained...

In summary, the Criminal Procedure Code gives search and seizure authority to the examining magistrate (2001), and Law 140 adds conditions to the authorization (2009). The E-transactions Law (2018) changes these conditions, and expressly states that the examining magistrate **and** the public prosecutor both have the authority to seize devices, whereas Law 140 states that the examining magistrate has the authority and the public prosecutor can only participate if asked by the magistrate.

This is where Judge Rabih Maalouf[23] (Misdemeanors Court of Appeal in Beirut) says we are on "dangerous grounds." The public prosecution can authorize the search without any limits or conditions stated in the law and without the need for justifications. This is a faulty procedure, considering that the public prosecutor is actually a party in the case, whereas the examining magistrate is considered a more independent entity. The public prosecutor could virtually give the authorization for any device search/confiscation. The examining magistrate, on the other hand, is the impartial party and their decision would be a more fair one.

In a discussion with Judge Maalouf, he suggested that the law should distinguish between the **entity that gives the authorization** and the **authority that actually proceeds with the search/seizure.** For example, the law could keep the decision in the hands of the examining magistrate and the execution in the hands of the public prosecutor, which would reduce the conflict of interest. Furthermore, the decision of the search and seizure would be better aligned with international standards and regulations.

23 Interview with Judge Rabih Maalouf, Misdemeanors Court of Appeal in Beirut

Jurisprudence concerning device seizures

Unfortunately, there has not been any precedent-setting jurisprudence concerning device seizures and their legal framework. However, there have been strategic litigations and judges' concurring opinions that highlight the issues with the legal framework concerning device seizures.

We will discuss strategic litigation efforts made by the Legal Agenda and the concurring opinion of Judge Maalouf.

In 2016[24], The Legal Agenda demanded the Public Prosecution (presiding Judge Samir Hammoud), to address the unlawful device searches, and stop the illegal practices committed by the judicial police and law enforcement. The Legal Agenda advocated for a circular that sets limits to abuses and urged the implementation of Law 140/1999 for the secrecy of communication, but the prosecution did not give any written answer. In response, The attorney general of the Court of Cassation said the public prosecution cannot issue a circular, claiming device seizures and searches are necessary in terrorism and drug cases, neither of which are clearly defined by the mentioned law (Law 140). The prosecution even refused to issue a statement for other crimes without any justification.

The Legal Agenda continued demanding an end to phone searches that violate the law by working on Strategic Litigation. Their demands were most of the time neglected or unanswered by the authorities.[25] One example is the Hammam Agha case in 2014 where the phones of 28 arrested people were searched based on suspicion of indecency. The Misdemeanors Court of Appeal in Beirut refused to consider a request to invalidate the device search because there was no explicit legal basis to invalidate it.[26]

The turning point was the decision from the Misdemeanor Court of Appeals in Beirut on 14/11/2018. The Court dismissed charges against three men who were accused of engaging in homosexual relations in violation of Article 534 Penal Code. Two of the defendants' identities were discovered with an unlawful device search by the police. The Court found that the men were not "caught in the act" of any unlawful behavior and did not convict them. Judge Maalouf went further in a concurring opinion about the unlawful device search.[27]

> "In a concurring opinion, Maalouf J further found the charges should be dropped as X's mobile phone was searched without a warrant, his right to the confidentiality of correspondence was violated, the investigation was marred by irregularities, and the alleged "evidence" was inadmissible as it was collected under duress and means of torture.
>
> [..] He was also forced to open his mobile phone for inspection by the police. Subsequently, two young Lebanese men who had contacted him via text through the dating app Grindr were subpoenaed for questioning. They were also interrogated about their private lives and their sexual orientation, but not assaulted, and were released a few days later.
>
> The Public Prosecutor's Office pressed charges based on the investigation claiming that the three young men committed the act of "unnatural sexual intercourse" under Article 534 of the Penal Code.[28]"

24 The Legal Agenda (LA) is a Beirut-based nonprofit research and advocacy organization with offices in Lebanon and Tunisia and correspondents in several other Arab countries. It was established in December 2009 by a group of legal professionals, scholars, and human rights activists who institutionalized their efforts to build a critical and multidisciplinary approach to law and justice in Arab countries with a special focus on political, civil, social, and economic rights.

25 غيدة فرنجية، 2019/05/04، مخالفة للقاضي ربيع معلوف: تفتيش الهواتف يتطلب إذنا من قاضي التحقيق، المفكرة القانونية – لبنان، متوفر على:
https://legal-agenda.com/مخالفة-للقاضي-ربيع-معلوف-تفتيش-الهوات/

26 غيدة فرنجية، 2014/09/02، المخالفات القانونية في قضية حمام الآغا: ملاحقة جماعية تنتهك حقوق الأفراد، المفكرة القانونية – لبنان، متوفر على:
https://legal-agenda.com/المخالفات-القانونية-في-قضية-حمام-الآغ/

27 Global Freedom of Expression Columbia University, X. v Public Prosecutor, Case N313/2015, Available at:
https://globalfreedomofexpression.columbia.edu/cases/x-v-public-prosecutor/

28 Ibid
Global Freedom of Expression Columbia University, X. v Public Prosecutor, Case N313/2015, Available at
https://globalfreedomofexpression.columbia.edu/cases/x-v-public-prosecutor/
Ibid

This decision is one of the first that tackles the legality of device seizures. Judge Maalouf refused to consider the proof presented, seeing that it was obtained from an unlawful device search, without any judicial or administrative warrant. He then argued that the prosecutor's decision is illegal, despite the fact that the E-transactions Law explicitly allows this practice.[29]

Judge Maalouf details the legal rationale behind his opinion by arguing that the Lebanese legal framework does not allow for this abusive search. He justifies his position with Article 2 of Law 140/1999 and Article 102 Criminal Procedure: there was no judicial authorization (Art. 2) given by the examining magistrate, who should have been the authority to give the authorization and not the public prosecutor (Art. 102).[30] Judge Maalouf also recalls the conditions cited in Law 140, which stipulates in cases of "extreme necessity" (حالات الضرورة القصوى), that the examining magistrate can authorize a device search, but his decision must be based on the persecution of a crime sanctioned by a minimum of one year of incarceration. The law also states the decision to authorize device searching must be written and reasoned, and it is irreversible. However, Judge Maalouf adds that the decision to search devices should be reversible just like search warrants for houses.

The judge also argues that in order to restrict a constitutional right, like the right to privacy, certain conditions must be met. The search of devices constitutes a breach of privacy (Article 12 Universal Declaration of Human Rights and Article 17 International Covenant on Civil and Political Rights) and it should only be restricted according to the law **(principle of legality)** and in case of necessity/serious crimes **(principles of necessity and proportionality).**

Ghida Frangieh tells us:

> "Device searching has become quasi-automatic in serious crimes regardless of the profile of the suspect. As for minor crimes, people from marginalized communities are more likely to have their devices searched. This is the case for example of low-income migrants and people suspected of sexual or morality offenses (including LGBTQ+ community) or drug users.
>
> It is in my opinion that device searches are often conducted without due respect to the principle of legality, necessity, and proportionality between the infringement on privacy and the need to protect public order."

As mentioned before, the legal framework does not apply when someone is called in for questioning prior to an arrest. Nazek Khatib, a public prosecutor, argues that the search and seizure of devices during questioning could constitute a threat to basic rights as the person summoned could be a victim of abuse.

29 Ibid

30 In an interview with Judge Rabih Maalouf about his concurring opinion he mentions the use of Article 102 and that this Article gives the authority for the authorization to the examining magistrate.

Article 102:
"The seals affixed to seized and kept items may not be removed except in the presence of the examining magistrate, their clerk, the plaintiff (or their personal representative) and the owner of the house in which the search took place or the person in whose presence the search took place. If any of the aforementioned individuals fails to appear, the seals shall be removed in their absence, provided that they had been notified of the date of this procedure.
The examining magistrate may view faxes and letters and keep any such items if they deem it necessary to uncover the truth or in order to prevent other parties from viewing them, if they believe that this would harm the investigation.
The examining magistrate may not disclose the contents of any seized fax or letter without the approval of its owner.
The examining magistrate may not view the correspondence between the defendant and their attorney."

Device seizures in the October Uprising

The device seizures that happened during the October 2019 uprising were mostly illegal or authorized by the public prosecutor. In fact, the majority of these searches happened after a notification (إشارة شفهية) from the public prosecution. Some even happened without any judicial decision or any authorization from the Administration, This is an important violation of privacy rights.

Most of the searches were authorized by the office of the public prosecution. In one case, the public prosecution ordered the ISF to search all devices from the 63 protesters that were arrested on January 14, 2020 (the "night of the banks") and those of the protesters in Tripoli on April 28, 2020. The decision also authorized the ISF to collect all the data from the phones.[31] Since 2018, the public prosecution can authorize device searching based on Article 123 of the E-transactions Law. The ISF has made a number of mass arrests since the October 2019 uprising in Beirut, especially in the Hamra area. However, on the night of January 14, 2020, the phones seized were transferred to The Cybercrime and Intellectual Property Rights Bureau[32] to pursue the investigation.

After the victims were released, most of them could not get their phones back unless they disclosed their passwords. If they did not comply, they were threatened with judicial persecution.[33] Some individuals who managed to get their phones back found modifications in the order of the applications on their phones, while others found new applications and some even got back phones that did not work at all.[34] A lawyer consulted SMEX to detect whether or not there had been any malware installed in one of these cases. SMEX's technical team did a quick forensics analysis on the phone to find that a breach of the phone was attempted with no success. This indicates that the privacy of the lawyer was breached without his consent, but no information was withdrawn.

The phones were used to track the protesters' locations during the protests in Hamra,[35] where protestors have congregated in front of and entered the Central Bank. The use of location services was combined with CCTV security footage from banks and streets to identify the protesters responsible for the "sabotage"[36] of the banks. Protesters expressed their frustration with the implementation of the capital control measures since the October 2019 protests, limiting their ability to access US dollars. The economic crisis also led to the uncontrollable depreciation of the Lebanese Lira, which is a result of years of corruption and negligent economic policies from the government, central bank, and private banks.

Diala Chehade,[37] lawyer and International criminal law expert also dealt with a case concerning a device seizure during the October uprising. The victim's phone was seized because he was passing through a protest. Chehade asked the Public Prosecutor to retrieve the phone for "professional reasons," since the victim needed the device for their job. Although she managed to retrieve the phone, this instance still demonstrates the lack of legality when it comes to device seizures. The Cybercrime and Intellectual Property Rights Bureau told

31 غيدة فرنجية، نور حيدر، سارة ونسا، 16-10-2020، كيف استخدمت السّلطة سلاح التوقيفات لقمع حرّية التظاهر والاعتراض؟، العدد 66 من مجلة المفكرة القانونية – لبنان "الثورة في مواجهة السّلطة وعنفها"، المفكرة القانونية، متوفر على: https://legal-agenda.com/كيف-استخدمت-السّلطة-سلاح-التوقيفات-لق/

32 The Cybercrime and Intellectual Property Rights Bureau, established in 2006, officially operates under the umbrella of the ISF but its legality is contested, given that it was established under a memorandum of service rather than by Law or Decree. The Bureau has been accused of acting as a censorship author- ity, mainly targeting journalists, bloggers and online activists. Its powers raise concerns as to the lack of safeguards protecting privacy and regulating the powers of the Bureau. On 2 October 2016 the leadership of the bureau changed after, Major Suzanne Hajj Hobeiche, the former bureau chief who had regu- larly targeted bloggers and activists, was asked to step down. Major Albert Khoury, a former lieutenant colonel in the ISF, replaced her - from : Privacy International & SMEX (2018, January), State of Privacy Lebanon. Available at: https://smex.org/wp-content/uploads/2018/02/State_of_Privacy_01_18.pdf

33 غيدة فرنجية، 2019/05/04، مخالفة للقاضي ربيع معلوف: تفتيش الهواتف يتطلب إذنا من قاضي التحقيق، المفكرة القانونية – لبنان، متوفر على: https://legal-agenda.com/مخالفة-للقاضي-ربيع-معلوف-تفتيش-الهوات/

34 غيدة فرنجية، نور حيدر، سارة ونسا، 16-10-2020، كيف استخدمت السّلطة سلاح التوقيفات لقمع حرّية التظاهر والاعتراض؟، العدد 66 من مجلة المفكرة القانونية – لبنان "الثورة في مواجهة السّلطة وعنفها"، المفكرة القانونية، متوفر على: https://legal-agenda.com/كيف-استخدمت-السّلطة-سلاح-التوقيفات-لق/

35 Ibid

36 Ibid

37 Interview with Ms. Diala Chehade, lawyer and international criminal law expert

Chehade and the victim that they went through with the seizure after getting authorization from the Public Prosecutor over the phone (mentioned above).

Chehade argues that the best chance for reform would be to fight for Article 47 (Criminal Procedure), since ensuring defense rights would automatically mean that no authority can proceed to a device search before the detainee is guaranteed the right for a lawyer.

The seizure of devices constitutes a breach of privacy and an infringement on basic rights, specifically the right to access information, communicate, and work. Furthermore, the seizures of these phones interrupted detainees' daily lives, which is especially inconvenient given the increasing cost of mobile phones amid the country's economic crisis.

Circular of General Prosecutor on December 3rd, 2019

Throughout the October uprising, the Thawra Hotline Lawyers,[38] and the Beirut Bar Association played a major role in strengthening defense rights for the arrested protesters, which led to the publication of circular No. 104/S/2019.

After pressure exercised by the Beirut Bar Association, the General Prosecutor (النائب العام التمييزي), Judge Ghassan Oueidat, issued a circular on December 3, 2019, to remind security officers of the detainees' rights and defense rights. Although there are gaps in circular No. 104/S/2019.[39] it constitutes an important "tool" in the hands of protestors, defense lawyers, and all residents in Lebanon. This is particularly important considering the general prosecutor supervises the work of the judiciary and the security agencies. The circular emphasizes the guarantees provided by Article 47 in the Criminal Procedure Code, specifically the right to remain silent, the need for a decision from the prosecution to keep detainees, and the obligation to remind the detainee of his/her rights.

In the second part of the circular, the prosecutor reminds us of the **"constitutionality" of the right to privacy,** especially when it comes to phones and the personal data stored on them. The prosecutor does not reference any legal text concerning privacy rights.

Basically, the circular "regulates" practice that should not be legal in the first place, instead of stopping it.

The circular did not ban the search of devices, but simply reminded the authorities to not delete the data "تفريغ المعلومات والبيانات" from devices. Nonetheless, illegal device searches have become more common among security agencies. They illegally examine data from devices as a means to pressure arrested victims and extract unlawful confessions. Moreover, as demonstrated above, a number of device seizures and violations of privacy continued to happen after the circular was issued.

In 2016, the Public Prosecution previously refused the Legal Agenda's demands to issue a circular concerning privacy rights and device seizures. Therefore, the General Prosecutor's decision to issue a circular during the October uprisings, albeit under pressure from the Thawra Hotline Lawyers and the Beirut Bar Association, represents a step in the right direction, but it is not sufficient to adequately protect people's rights.[40]

38 Lawyers defending protesters, victims of police brutality, arrests, summons, labour law and banking issues. They have been coordinating and helping protesters since the 2015 Tol'et Rihetkon movement and during the October 17 uprising in 2019.

39 Ta'mim li-Oueidat Yata'allaqu bi-l-Madda 47 min Usul al-Muhakamat al-Jiza'iyya wa-Damanat Himayat al-Mushtabah fihim", 3/12/2019, National News Agency's website, Available at: http://nna-leb.gov.lb/ar/show-news/449924/nna-leb.gov.lb/nna-leb.gov.lb/ar

لور أيّوب ، غيدة فرنجية، 2020/10/21، محامو لجنة الدفاع عن المتظاهرين: أيّ تصوّرات لدورهم ودور نقابتي المحامين؟، العدد 66 من مجلة المفكرة القانونية – لبنان، المفكرة القانونية، متوفر على: https://legal-agenda.com/محامو-لجنة-الدفاع-عن-المتظاهرين-أيّ-تص/

40 غيدة فرنجية، 2020/10/01، معارك المادة 47: كيف انتزعت الانتفاضة حقوق الدّفاع للمحتجزين؟، العدد 66 من مجلة المفكرة القانونية – لبنان، متوفر على: https://legal-agenda.com/معارك-المادة-47-كيف-انتزعت-الانتفاضة-حق/#_ftn14

Conclusion & Recommendations

In conclusion, the Lebanese legal framework is vague and not suitable for the protection of privacy rights. Concerning device seizures, the authority to permit the seizure and the search lies in the hands of the judiciary (examining magistrate) or the Administration (Law 140). Since the E-transactions law in 2018, the public prosecutor has the authority to order a seizure too. We still do not have relevant jurisprudence when it comes to the subject. Currently, the Lebanese authorities do not value freedom of expression and privacy rights. This could lead to increased surveillance and indicate the transformation of the Lebanese state into a police state. We provide the following recommendations:

1) Amend Article 123 of the E-transactions Law to add restrictions on personal device searches similar to the restrictions included in Law No. 140/1999. This aims to subject the search of devices to the procedures related to the search of private communications, rather than the search of objects.[41]
2) Request the general prosecutor to issue clear instructions on conditions for device searches and seizures that respect the principles of legality, necessity, and proportionality of the infringement on privacy.[42]
3) Transfer the authority for judicial orders exclusively to the examining magistrate, also known as the investigative judge, because the public prosecutor is still a party in litigation, which could lead to biased orders
4) Develop accountability mechanisms to ensure that security agencies are respecting laws and regulations.
5) Continue the fight for defense rights, and the enforcement of Article 47 Criminal Procedures Code in front of all jurisdictions.
6) Phones and other devices should not be taken when individuals are summoned for questioning unless there is a judicial order

39 Interview with Ms. Ghida Frangieh, Lawyer at the Legal Agenda
42 Ibid