Building Trust: Toward a Legal Framework that Protects Personal Data in Lebanon

Baseline Study by the SMEX Fellowship for Reporting on Digital Freedoms

SMEX

www.smex.org
www.facebook.com/smex
www.twitter.com/smex

SMEX Fellow: Elham Barjas

SMEX Fellow: Hussein Mehdy

Managing Editor: Lara Bitar

Consulting Editor: Mohamad Najem

October 5, 2017

Authors: Elham Barjas (sections 1 and 4) and Hussein Mehdy (sections 2 and 3)
Contributors: Sara Rammal (author of the introduction) and Dr. Pierre Khoury (author of the conclusion)
Translator: Nadine Saliba
Graphic Designer: www.salamshokor.com

A 2017 Publication of SMEX
Kmeir Building, 4th Floor, Badaro, Beirut, Lebanon

Table of Contents

About this Report

The lack of a comprehensive legal framework for privacy rights and data protection in Lebanon has led to the adoption of illegal mass surveillance programs and to the violation of individual and collective privacy without repercussions. In order to understand the mechanisms under which surveillance is conducted in the country, to identify areas in need of reform, and to devise strategic advocacy for privacy protections, SMEX issued its inaugural report on digital surveillance titled "Mapping the Landscape of Digital Surveillance in Lebanon" on December 14, 2016.[1]

Having developed a foundational knowledge base on issues related to privacy, surveillance, and data protection, SMEX designed a program — the SMEX Fellowship for Reporting on Digital Freedoms — to promote, facilitate, and disseminate research on digital rights in Lebanon, with the aim of providing evidence to enhance public discussions surrounding these issues.[2] The fellowship provides an opportunity to develop skills, expertise, and knowledge on digital freedoms-related issues in the Middle East and North Africa (MENA).

This report is the product of our call to journalists, human rights activists, and researchers to conduct further investigations and research into the state of digital rights in Lebanon — under the guidance of the SMEX Fellowship for Reporting on Digital Freedoms.

Executive Summary

The Lebanese state is increasingly relying on digital technologies in its collection and storage of personal data. It has already started to issue biometric passports and smart biometric residence permits, and to convert driver's licenses to biometric ones. The Communications Minister has proposed linking individuals' phone numbers to their IDs through a specialized private company. It is clear that the government is trying to grow its use of new technologies to collect personal data through private companies.

However, the Lebanese state is embracing these new technologies and adopting these new policies without clear guidelines to protect the data it is amassing and without privacy guarantees. This is particularly troubling in light of several cases of data leaks, some of which are known to the Lebanese public while others remain unreported.

This rapid adoption of new technologies without any safeguards led SMEX to conduct a study on the regulatory framework for data protection, especially its legislative and technical aspects, which deal with personal data belonging to Lebanese citizens and people residing on Lebanese soil — to assess its strength and weaknesses. This assessment requires shedding light on both the legislative framework for personal data in Lebanon and the technological mechanisms employed by the relevant authorities to provide data protection. It also requires highlighting cases that justify the mounting questions and skepticism regarding the efficacy of the existing systems, both legal and technological, given that violations of the privacy of different groups of individuals have repeatedly taken place.

In its first section, the study examines the legal framework regarding personal data in Lebanon. Even though Lebanon participated in developing the directives on data protection legislation issued by the United Nations Economic and Social Commission for Western Asia (ESCWA) in 2012, the country still lacks specific legislation on personal data. At the time of publishing this report, the Lebanese legislature has not issued any legislation in this regard, but has held general discussions on the legal definition of personal data and suggested a theoretical framework to process it.

In its second section, the study defines biometric data, explains the technology employed in collecting it, and summarizes the most important methods used to encrypt and protect it from breaches. The study highlights the use of biometrics given recent technological advances and discusses the importance of using sophisticated protections to ensure that data is protected from leaks and breaches. The report summarizes and evaluates the recent adoption of biometric passports and residence permits by the General Directorate of General Security. Additionally, it highlights the types of data the authorities are storing relating to both Lebanese citizens and foreign residents, especially since the Directorate has unhindered access to this data.

In the third section, the study reviews data leaks originating from different sectors, underscoring the extent to which Lebanese citizens and residents' personal data is being misused. The study reveals that personal data collected in the country is susceptible to infiltration and to leaks due to weak protection systems and the absence of specialized legislation.

In the fourth section, the study reviews the "Electronic Transactions and Personal Data Protection" draft law, which a subcommittee formed by the joint parliamentary committees is currently discussing. This draft law includes a complete section on the protection of personal data. However, since the bill is yet to become law, this study examines articles that protect personal data scattered among different Lebanese laws. It also scrutinizes and evaluates the draft law in light of foreign legislation, especially French law, which has informed the Lebanese draft law and the ESCWA directives with which the Lebanese law should be compatible. In addition, the study highlights the role of the Information and Communication Technology Center at the Beirut Bar Association in improving the bill through its participation in the ongoing discussions held by the subcommittee.

Introduction

"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say," according to National Security Agency (NSA) whistleblower Edward Snowden, who leaked information exposing secret US government mass surveillance programs. How valid is this statement in light of recent technological developments that have eroded fundamental human rights and freedoms?

Apart from the legal issues, and from a purely social perspective, what would happen if people—who have nothing to hide—are approached by strangers on the street and asked their names, phone numbers, and bank account numbers? What if they were asked about the places they visited, the illnesses they have, their psychological, emotional, and physical state, or their religious beliefs? The ability to easily access this kind of information without consent constitutes a violation of the right to privacy and fails to preserve the inviolability of personal data. Otherwise, why would people refuse to share their personal information with strangers, or the details of their personal and intimate lives with their neighbors and colleagues? While these individuals have the choice to decline answering these intrusive questions, surveillance systems have made protecting our private and personal information increasingly difficult.

Collecting and processing personal data have created new challenges to the right to privacy, partly because digital data legislation in some countries has not kept up with these rapidly evolving technologies, especially in third world countries like Lebanon.

Personal data protection and individual privacy are under threat globally as a growing number of states are acquiring the ability to have unrestricted access to their residents' digital communications and personal data. This infringements on privacy rights are justified under the pretense of maintaining security, combating terrorism, and fighting crime, including organized crime carried out online and offline. This is also true in the case of Lebanon, which has imported illegal mass surveillance technology with little to no transparency or accountability.

The absence of legislation that keeps pace with technological developments has hindered Lebanon's ability to protect personal data from arbitrary and illegal practices, from both state and non-state actors. Furthermore, monitoring personal data exchanged through digital means often makes it possible to draw a clear picture of individuals, their movements, the nature of their communications, and their relationships. For this reason, the unregulated collection of personal data not only restricts the right of an individual to express themselves and to communicate their views freely without fear of facing condemnation, but also violates their right to privacy as their data, movement, or messages are intercepted, collected, analyzed, and sometimes exploited by government agencies, institutions, and private companies. Achieving a balance between the right to access and share information on one hand and the right to privacy and personal data protection on the other is a necessary project that the current draft law on personal data does not adequately address.

Our rights are interconnected and obstructing the exercise of one right may constitute a threat to another. This report is the first step in the study of the Lebanese legal framework for the protection of personal data in light of constitutional articles and various international treaties binding the Lebanese state. These include legal provisions scattered in more than one Lebanese law (especially the Penal Code, the Banking Secrecy Act, the Code of Medical Ethics, the Consumer Protection Act, the Code of Criminal Procedure, etc.). They also include Law No. 140/1999 on wiretapping, which protects communications, local and international, conducted through any medium, whether wired or wireless (landlines, mobile phones, fax , email, etc.).[3] By outlining the current legal framework, this study aims to help advance legal reforms that specifically address the importance of data protection legislation.

Section 1: Legal Framework

To date, the Lebanese legislature has not proposed a definition for personal data or the processing of personal data, nor has Lebanon paid particular attention to the protection of personal data at the legislative level. The parliamentary subcommittee, formed by the joint parliamentary committees, has only recently begun to discuss the "Electronic Transactions and Personal Data Protection" draft bill. Section V of the draft law is entirely devoted to the protection of personal data.

• Defining Personal Data and Data Processing

Most pieces of legislation on personal data derive from the European convention on the protection of personal data (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data). The Lebanese draft law contains a definition informed by French law and is in compliance with the European convention. However, the draft law diverges from international standards when it comes to regulations on data processing.

The Lebanese draft bill defines personal data as "all information relating to a natural person that enables their identification, directly or indirectly, by comparing and cross-referencing information from multiple sources." This definition corresponds to the text of the French law, as the Lebanese draft law derives much of its provisions from the French law when it comes to personal data.[4]

In general, definitions of personal data are similar across various laws. For example, the African Union's Convention on Cybersecurity and Personal Data Protection adopts the same definition. This similarity exists because all these texts have used the European convention as a reference on personal data protection.

The European convention defines personal data as "any information relating to a natural identified or identifiable individual." The Framework Decision 2008/977 issued by the European Union (EU) in 2008 "on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters," added the following to the European convention's definition of personal data "data specific to a person's physical, physiological, mental, economic, cultural, or social identity."

Therefore, any proposal on the definition of personal data must take into account the broader and more comprehensive definition employed at the international level. After all, Lebanese legislation is intended to protect personal data, and since matters related to digital technology are international in scope, personal data is defined as:

> *All information relating to a natural person that enables their identification, directly or indirectly, by comparing and cross-referencing information from multiple sources (according to the Electronic Transactions draft Bill), and pertaining to a person's physical, physiological, psychological, economic, cultural, and social identity.*

This definition meets ESCWA's cyber legislation directives issued in 2012 in Beirut under the project Regional Harmonization of Cyber Legislation to Promote the Knowledge Society in the Arab World.[5]

Processing personal data poses a serious threat to data security, so it is central to any legislation concerned with data protection. As such, the definition adopted by any law should reflect the legislators' commitment to ensuring the broadest possible data protections.

The "Electronic Transactions and Personal Data Protection" draft bill defines data processing as "any operation or set of operations related to the data, regardless of the procedure used, especially collecting, recording, retention, adaptation, alteration, retrieval, use, transmission, dissemination, deletion, destruction, or any other form of making the information available." This definition not only conforms to the French law,but it also complies with the ESCWA directives.[6]

Both the Lebanese and French texts incorporate definitions of "the controller of personal data" and "the recipient of personal data." It should be noted that the French text is more detailed, but the two texts still share many similarities. According to the Lebanese draft law, the two entities can be defined as follows, "a data controller is any person, public authority, or body that determines the purposes and means of processing."

The French legislator on the other hand, did not just refer to "a natural person or a legal person," but enumerated the parties that could be subject to the law in their capacity as data controllers. They are, "a person, public authority, or body that determines the purposes and means of processing."

The recipient of personal data is an authorised person other than the data subject (the individual about whom the data is processed), the data controller, or the data processor (the individual in charge of processing the data) to whom the data is disclosed. Public authorities legally authorized, for a specified purpose, to request personal data are not deemed to be the recipient.

● How Lebanese Law Protects Personal Data

There are no safeguards regarding personal data protection under the laws currently in force in Lebanon, except for some articles scattered among various laws. Nevertheless, the state is increasingly collecting and processing data. It is doing so by contracting with local and foreign private companies, adding an additional layer of vulnerability to individuals' right to privacy.

Lebanese pieces of legislation contain many articles related to information security and cybersecurity. They mostly protect individuals' right to privacy as the entity concerned in each law protects the confidentiality of their data; however, aside from the right to privacy, few of these texts address other rights related to personal data.

Lebanese Laws on Personal Data Protection

A. The Right of Access to Information Law
Articles 4 and 5 of the Law enshrine the right of individuals to access data collected by the administration (public entities and a limited number of private entities, notably those that are controlled by a public entity; that participate in the provision of a public service; or that are in the management of public property), or any of the parties subject to the provisions of said law.

According to Article 4, "the interested person shall have exclusive access to personal files and any evaluative reports pertaining to a natural person referred to by name, identification number, code, or other identifying features such as fingerprints, eye, voice, and image recognition."

"Personal files shall mean personal status records and files containing all information pertaining to a natural person, directly or indirectly, including the IP address, by comparing or cross-referencing information from multiple sources."

"The interested person shall have the right to request correction, completion, updating, or deletion of personal information related to them in the event that it is incorrect, incomplete, ambiguous, outdated, or is the kind of information prohibited from being collected, used, exchanged, or retained."

Article 5 excludes a range of information from the previous article, including the private life of individuals, their mental and physical health, and secrets protected by the law, such as professional and trade secrets.

B. The Consumer Protection Act (Article 58)
This law requires the supplier (i.e., businesspeople, industrialists, craftspeople and service providers) to conceal and protect the information it has obtained, unless the consumer has expressly agreed otherwise. The Consumer Protection Act regulates the medical profession, but also requires the supplier to "take all measures necessary to keep such information secret." The provisions of this law are subject to a special body called the Dispute Settlement Committee.[7] This committee follows brief procedures and exempts a review claimant from having to appoint a lawyer. It also allows civil society organizations to file suit to rescind arbitrary clauses included by companies in their contracts. For example, it allows organizations to challenge clauses that enable a company to use individuals' personal data without their prior consent. In other words, there has been some progress on the protection of personal data, pending the passage of a specialized legislation.

C. Decisions, Regulations and Circulars on Data Protection Issued in 2000 by Banque du Liban
For example, Circular No. 134 dated February 12, 2015 states that Banque du Liban is committed to "Protecting the customer's personal and financial information, without prejudice to the legislation in force, particularly the Banking Secrecy Law and Anti-Money Laundering Law." Decision No. 7548 on Electronic Financial and Banking Transactions issued on March 30, 2000 stipulates in Article 12: "To obtain

authorization from Banque du Liban for electronic cash transfers, [Lebanese institutions] should file a request accompanied by (...) documents pertaining to the work systems and technical rules they intend to follow in carrying out their electronic operations and that demonstrate they have an effective electronic protection system for their operations..."

Lebanese Laws on the Right to Privacy

A. The Telecommunication Interception Act
It regulates the interception and surveillance of communications.[8]

B. The Telecommunications Law
It imposes an obligation of confidentiality on everyone engaged in inspection and control within the telecommunications sector (Article 38).[9] The article states:

"Controllers and inspectors may enter all public and private properties where it is necessary for them to execute their official duties and in order to inspect or collect information related to existing or planned facilities and installations, review records and documents and extract copies thereof, and request presentation of any useful document or information. Provisions of the Penal Procedure Code and procedures of the judiciary police force will govern cases of forced entry and issue infringement reports whenever there is sufficient evidence indicating an infringement."

The information that inspectors and controllers become aware of in the course of carrying out their duties is considered confidential and may only be disclosed to their direct superiors or upon the request of the competent judicial authorities. These rules of confidentiality shall apply to all persons who are privy to such information by virtue of their work at the Telecommunications Regulatory Authority (TRA) or the Ministry.

C. The Banking Secrecy Act
Under this Law, issued on September 3, 1956, banks are not permitted to disclose banking secrets to private entities or public authorities, whether judicial, administrative, or financial, except in cases specifically defined by the law.

D. The Lebanese Penal Code (Articles 579, 580, 581)
This law punishes "anyone who, by virtue of their position, profession, or art, is aware of a secret and discloses it without a legitimate reason ..."

It's important to note that a 'legitimate reason' may include orders received by the employee from their direct superiors. This leads to impunity as the employee escapes punishment in the absence of a clear system that specifies the parties entitled to access and request an individual's data. In addition, these articles apply to employees of the Ministry of Post and Telecommunications who misuse their powers and violate the confidentiality of the data of those benefiting from the services of these agencies. It should be noted that these articles, in terms of their formulation and content, are suited to traditional, pre-electronic means of communications. They do not keep up with technological advances. To be effective for this day and age, Lebanon needs progressive judicial interpretation to reinterpret the legal texts.

E. Code of Medical Ethics (Articles. 6 and 44)
Article 6 states that "the professional secrecy which binds Physicians is subject to exceptions prescribed by the laws." Article 44 refers to the duty of a physician charged with medical supervision by a certain administration to "maintain professional secrecy and only give information of administrative nature or use without revealing the medical reasons for that. A physician is also prohibited from providing medical information available in medical files to any other person or administration, except as stipulated in the general laws."

These articles provide solid legal guarantees with respect to individual medical information. But alone, they remain insufficient in light of current technological developments. These developments compel hospitals and physicians to apply clear standards to protect their patients' files from any possible electronic breach. Physicians and hospitals are held responsible for leaks in patient data if they do not comply with these standards. The Order of Physicians must play a central and pioneering role in this regard.

International Laws and Regulations Binding the Lebanese State

To date, Lebanon has not signed any international convention on the protection of personal data. Therefore, the Lebanese state is only committed to the general principles of personal data protection at the international level. United Nations (UN) resolutions include the most important of these principles and the Lebanese constitution requires Lebanon's adherence to the UN Charter and the Universal Declaration of Human Rights.

Protection of personal data falls under UN resolutions on the right to privacy, most notably UN General Assembly resolution 86/167. As a co-sponsor of that UN Resolution and Resolution 166/69 adopted in December 2014, Lebanon is committed to promoting, respecting, and ensuring the right to privacy as a human right.[10]

At the regional level, the Arab Center for Legal and Judicial Research is developing a draft of an Arab agreement aimed at "building confidence in cyberspace," with a section devoted to "protecting personal data."[11] The adoption of this agreement by the Arab League will create a legal framework for the protection of personal data in the Arab region. This step is in line with the international trend towards drafting legislation suitable for the transboundary nature of cyberspace.

However, the Lebanese state is committed to a series of regional conventions on security that make the protection of personal data and the status of data subjects more vulnerable as compliance with these conventions is not accompanied by any national legislation to protect, organize, transfer, or process this data. One of the most prominent conventions is the Arab Convention on the Suppression of Terrorism, which Lebanon joined in 1999 by virtue of Law No. 57 issued on March 31 of that year.[12] The law contains provisions urging signatory states to establish databases and to exchange information amongst themselves with respect to anything they believe is linked to combating terrorism, which may lead to the prosecution and persecution of individuals on the basis of their political views.

To recap, Lebanese law contains a number of scattered articles that protect personal data in many sectors. However, Lebanese legislation lacks a specialized law or bill dealing with the protection of personal data in a comprehensive manner. This legislative gap continues at a time when security and counterterrorism are used as pretext for violating people's data and their right to privacy. While these measures may be necessary to preempt terrorist operations, they are often used to harass people in general and human rights activists in particular, under the pretext of maintaining security.[13] This ambiguity highlights the need to expedite the passage of a law regulating the processing and protection of personal data.

Section 2: Biometric Data - The Latest Digital Technology Used by the Lebanese Authorities

• Definition of Biometric Data

Biometrics is a term derived from the Greek words 'bio,' which means life, and 'metric,' which means to measure.[14]

Biometrics is the science of automatic verification of human identity through the composition of the human body, that is, by measuring the statistical analysis of the physical and behavioral characteristics of individuals. This term is used to refer to data about individuals collected through their biological or physiological characteristics, such as iris and retinal scanning, fingerprint, face and voice recognition, hand geometry, and DNA.[15]

The importance of using this technology lies in the possibility of verifying the identity of each individual automatically through the biometric authentication of their physical and behavioral characteristics since every individual has distinct physiological and anatomical characteristics that are unlike those of any other individual. The eye is one of the most important physiological features, as it is almost impossible to change.

All biometric systems work in the same way. They process, through programming and encryption, the unique features of each person and store them in a database. There are two main types of biometric identifiers:
- Physical characteristics: shape or composition of the body (fingerprints, DNA, face, hand, retina, iris, etc.).
- Behavioral characteristics: the person's behavior (rhythm, gait, gestures, sound, etc.).[16]

• Biometric Authentication

After collecting biometric data and storing it in a database, the individual is asked to verify their identity. When providing their biometric data to the machine, the data is recorded and compared with the record stored in the database. If the data matches, the identity of the person is confirmed.[17] Some biometric identifiers, such as keystrokes or walking in real time, can be used to provide continuous authentication rather than a one-time authentication. Methods of authentication through the iris and pattern of the retina can be used in some ATM machines, while companies use hand geometry technology or fingerprints to record the time and date of employee entry and exit in and from work. A large number of security agencies around the world use face recognition technology, particularly for identifying people in large crowds.[18]

• Biometric Data Encryption

Defining Encryption

Encryption is the conversion of electronic data into another form, called ciphertext, which cannot be easily understood except by the party that encrypted the data and those authorized to access this data.

The primary purpose of encryption is to protect the confidentiality of digital data stored on computer systems or transmitted over the internet or other computer networks. Modern cryptographic algorithms play a vital role in ensuring the security of Information and Communications Technology (ICT) systems.[19]

Technology Used in Encryption

Information security expert Elie Nasr[20] explains the two basic encryption technologies:
1. Symmetric Encryption, whereby information is encrypted and decrypted by a single key, a technology often used by security agencies in most countries.
2. Asymmetric Encryption is a technology that uses two encryption keys, one public and the other private, whereby data is stored when recorded with one key and decrypted with the other. Only someone who has the private key can decrypt the encrypted data. This method is used, for example, by websites on which people engage in selling and buying operations using credit cards, websites that users access by entering passwords for the website account, or email accounts. This technology relies on a third party that has the encrypted data to guarantee the safety and security of personal data.

The Directorate of General Security began using smart biometric residence permits in 2017,[21] although the decision was taken back in 2014.[22] Between 2014 and 2017, the Directorate issued several statements about these residence permits and the need to use them. The Directorate also began issuing biometric passports in August 2015,[23] in compliance with the standards imposed by the International Civil Aviation Organization (ICAO),

as the Directorate itself indicated.[24] At the time, a decision was issued by the Directorate of General Security to replace current passports with biometric ones within a short period.[25] The decision was accompanied by widespread rumors that some countries are going to refuse entry to people traveling with non-machine-readable passports.[26] Not to mention that the statement issued by the Directorate of General Security toward the end of 2015 lacked adequate clarification. It only pointed out that in order to travel, people need to replace handwritten passports, or passports listing the names of accompanying persons.[27]

Lebanon was late in meeting its international obligations. The Lebanese state had been notified on December 31, 2012 of the ICAO decision, namely, that November 24, 2015 was the deadline for phasing out non-machine-readable passports. However, the state refrained from suspending the use of non-machine-readable passports, then abruptly took the decision to do so. This led to ruminations on whether the decision had anything to do with biometric passports.[28]

The head of the Office of Nationality, Passports and Foreigners in the Directorate of General Security, Brigadier-General Hassan Ali Ahmad, said in an interview with the General Security Magazine, that in early 2016, some countries declared their commitment to the standards issued by the ICAO and began refusing any non-machine-readable passports.[29] Their decision would apply to Lebanese passports that included a list of persons accompanying the main passport holder. Brig. Gen. Ahmad made mention of Directorate of General Security's previous request to replace these passports.

But why did the Directorate of General Security surprise the Lebanese people with the news, limiting the timeframe to renew their non-machine-readable passports, even though the ICAO had announced on December 31, 2012 that the deadline for phasing out non-machine-readable passports was November 24, 2015?

According to the Directorate of General Security, its decision coincided with notifications about the need to renew passports, received by Lebanese missions abroad, as states began to gradually comply with the demands of the ICAO. That is why the Directorate of General Security's decision was hastily issued on December 24, 2015. Its main concern, said Brigadier General Ahmad, was to prevent travellers from facing problems overseas. The Directorate of General Security held the media responsible for the confusion that ensued due to their inaccurate reports on the subject.

The adoption of biometric passports began in August 2015. The Lebanese Ministry of Interior, in agreement with the Directorate of General Security,[30] granted Gemalto, a company based in Amsterdam,[31] a contract to provide a surveillance system for entry at airports, seaports, and land border crossings. Additionally, it granted Inkript, a Lebanese company owned by Hisham Itani, a contract for biometric passports.[32] It must be noted however, that the Dutch company's data had been hacked by American and British spy agencies, namely, the US National Security Agency (NSA) and the British Government Communications Headquarters (GCHQ).[33]

Biometric Passports

According to the International Organization for Standardization (ISO 19794), a biometric passport is an electronic passport containing electronic chips that include information about the passport holder, the individual's digital photo, and their fingerprints.[34] The Directorate of General Security may later add any biometric information they deem necessary onto these chips.

This electronic chip is linked to an encrypted information system, and the Directorate of General Security is the only party that can access this information. Biometric information collected from residents in Lebanon is the same as that collected for biometric passports, but it also includes basic information about a residence permit holder in addition to their photo and fingerprints.[35]

SMEX sent inquiries to the Lebanese government, asking about the systems its institutions use to protect data. How is data stored, who is entitled to access it and how is it encrypted and protected? SMEX asked these questions as they relate to biometric residence permits as well.

In addition to the previous questions, SMEX has asked the Directorate of General Security additional questions about the coordination between the Lebanese state and countries of foreign nationals residing in Lebanon, inquiring specifically about the level of information exchanged between them, and requested details about the coordination with the UN High Commissioner for Refugees (UNHCR). SMEX also asked to meet with any of the officials in charge of this issue. However, the Directorate responded with a brief letter indicating that the new

passports contain mechanisms for safety and trust and are impossible to falsify. According to the letter, smart biometric cards constitute a "technological and organizational development consistent with the Directorate's policy of constantly developing its work." The letter pointed out that coordination with UNHCR is carried out through special mechanisms and a memorandum of understanding signed in 2003, adding that the biometric residence permits register all eligible foreign nationals, including Syrians who have met the conditions of residency.

The Directorate of General Security did not provide an answer regarding the technology they use to encrypt data. However, based on his knowledge and familiarity with the technology used in many countries around the world, Elie Nasr suggests that the Directorate of General Security likely uses the first type of encryption technology. He added that it might use the second type of technology to transmit data over the internet or through a network connecting different agencies and centers, but it probably sticks to the first technology for the encryption of basic data.

A passport can be forged, and the chip attached to it can also be imitated, but fraud is detected when the passport code and the code saved in the General Security files are compared. The information attached to the chip constitutes a special code for the the passport holder and is only known to the Directorate of General Security. To prevent forgers from detecting the code by using the same methodology used by the Directorate of General Security in creating the code, the latter has to add numbers or symbols to the data, thus making forgery a very difficult task unless the data is leaked from the Directorate of General Security itself.

Nasr points out that machine-readable passports and biometric passports are not different in terms of data storage, or encryption. However, biometric data makes the automatic identification of individuals possible and the Directorate of General Security can attach any additional data it wants to the basic data collected about individuals. The Directorate can also specify the information that General Security personnel are allowed to see at border crossings or in their offices as well as the information prohibited from being accessed.

Residence permit data is stored on a different server than the one where passport data is stored, but the storage technologies adopted are the same and only vary slightly in encryption methods. The Lebanese government can exchange this information with other countries through an agreement between the two states, such as the Arab Convention against Terrorism. According to the Convention, each signatory state commits to provide all other signatory states with information and data available to it that could contribute to fighting terrorism. Among the data that could be exchanged is "the description of a wanted person with the utmost possible accuracy and any other data that might identify a potential terrorist and that individual's nationality and identity." Each signatory state shall, in accordance with Article 3 of the Convention, establish a database for the collection and analysis of information on terrorist individuals, groups, movements, and organizations and stay abreast of the latest developments in matters of terrorism including successful cases of confronting it. In addition, states should update this information and provide it to specialized agencies in other signatory states, in accordance with the confines set by the national laws and procedures of each country.

Adoption of Biometric Passports and Residence Permits

Information is exchanged through an information program used by the Lebanese state (different from the one used to store residence permit data), whereby another state is given access to specific information that the authorities place on the server, which is periodically updated. Technically, the process is quite simple. It is enough for the program to have a barcode or a chip-reading feature.

In the absence of a law regulating the encryption and storage of biometric data, and given the weak legal protection of personal data in Lebanon, encryption of information is nothing more than a measure to protect this information from hacking. But encryption cannot guarantee the protection of private data unless there are laws and procedures in place protecting this data against any violation of the right to privacy and the right to protect personal data by the official agencies themselves.

Section 3: Recent Violations and Misuse of Personal Data

• Hospital Patients' Data

In April 2012, the administration at the American University of Beirut (AUB) asked the university's information department to obtain all the data stored on computers, both on campus and in the medical center. The information department objected at the time because the data included all electronic correspondences between everyone at the university — from faculty to students and staff — through the institution's email, which ends with «aub.edu.lb». The administration's request also included employees' personal and professional information, as well as very sensitive information belonging to physicians, staff, and patients at the American University Hospital (AUH).[36]

The administration wanted this data because sensitive information about the university and the policy adopted by its administrators had been leaked, which it believed was quite damaging. So it requested the data to find out who was leaking information about the university and its secret business discussed over the email server.[37]

At the time, several questions were raised about the fate of this data and regarding the level at which it is protected. After all, the university itself had noted that "the technical environment at AUB is not secure."[38] The university's database, including data from AUH, was moved from one department to another, but the leaks continued.[39] (Full disclosure: Hussein Mehdy, one of the authors of this report, played a role in highlighting these leaks by publishing some of the data in a Lebanese newspaper,[40] revealing cases of waste, corruption, and mismanagement at AUB and its medical center.[41])

These repeated leaks raise serious questions about the systems used to protect the data of patients who go to AUH as well as other hospitals. AUB's medical center, Beirut Governmental Hospital, and Hotel-Dieu de France hospital did not respond to SMEX's inquiries regarding the safety of their patients' data. The information department at Mount Lebanon Hospital said that this information is confidential, adding that they cannot disclose the name of the program they use nor comment on whether it is secure or not.

Fear that the system could be breached gives rise to these questions. The most recent report about the information leaks at AUB was an unpublished report issued by FTI Consulting, stating that the information system at the university is fragile and that they could not find the source of the leak. In fact, one of the authors of the report obtained medical files from AUH after they learned that the system had been breached, confirming that this data, which is supposed to be protected by the applicable laws, is actually not protected at all and patient privacy is at risk. The party that stands to benefit the most from these leaks, according to sources within the university, are the insurance companies that try, any way they can, to know all the details about the health of their clients. Commenting on the issue, the head of the National Association for Social Health, Dr. Ismail Sukkarieh, said that if this data reaches insurance companies, it could affect the relationship between the company and its clients. For instance, a company might refrain from renewing an insurance policy, or raise the premium on a patient if it finds out from a medical file that its client has or is prone to chronic diseases or an illness requiring costly treatment.

• Personal Cell Phone Numbers

Citizens and residents of Lebanon receive text messages, also known as SMS (short message service), and emails from dozens of businesses, associations, institutions, municipalities, individuals and others on a daily basis, without having granted them permission to do so.

Mobile phone operators in Lebanon do not provide a service that prevents all commercial text messages from being sent. They do, however, provide a service that prevents a text message from being sent again from the same source. The activation of this one-time service, however, requires a subscriber to contact the mobile operators' representatives and provide them with the name and number of the sender, as was confirmed to SMEX by the representatives of the two cell phone companies when SMEX called the customer service number 111.

However, the operators sell their users' data to business and other interests. During the course of preparing this report, SMEX found out that the average cost of sending 1,000 text messages is about 45 USD and it costs up to 11,000 USD to send 500,000 text messages. The average cost of sending 50,000 emails is 150 USD, while the average cost of sending 360,000 emails is 430 USD.

Text Messages	Cost (USD)	Emails	Cost (USD)
1,000	45	50,000	150
5,000	150	100,000	270
10,000	300	160,000	290
50,000	1,300	360,000	430
100,000	2,500		
500,000	11,000		

The Lebanese people's data is for sale at the hands of the two cell phone companies, touch and Alpha, advertising companies that offer the service of sending text messages or emails depending on the client's request, and advertising companies specialized in sending this type of messages. The two cell phone companies admit selling their subscribers' data to businesses or individuals who want to send text messages to a target group as defined by gender, age, and profession, according to the websites of both Alpha[42] and Touch.[43] This is data that the companies obtain the minute people purchase prepaid lines, make their lines postpaid, or when their employees call customers.

Another dubious method, dividing consumers into target groups, offered by touch enables ad companies to send messages based on the information it provides, such as "usage behavior," and other private data. How does touch store this data, and why does it store data on "usage behavior" with the intention of selling it? What are the procedures used by the two mobile companies to protect this data from being leaked, and do the advertising companies that offer SMS purchase this data from the two mobile companies? This is especially peculiar as most of the ad companies claim to use the two mobile companies to send their messages. SMEX sent these questions to Alpha and touch, but did not receive a response from either.

In an interview with SMEX, attorney Tony Mikhail said that Law 431/2002, which regulates the telecommunications services sector, did not address in any of its articles the protection of personal data. Mikhail pointed out that the Right of Access to Information Law, which was recently passed by parliament, protects the data of the Lebanese people, but this protection is limited to preventing public institutions from providing anyone with private and personal information about Lebanese citizens. So even if it is implemented, the law only addresses a small percentage of violations against the right to protect personal information.

SMEX contacted several, randomly-chosen advertising companies that provide the same service (the selling of personal data), asking for a list of prices for the services offered and inquired about other aspects of their work. All the companies SMEX contacted said that customers can choose the age group, gender, place of residence or place of registration, profession, and other personal data about individuals, but refused to disclose whether they get this data from Touch or Alpha.

The company, Bestsmsbulk, allowed SMEX to use a demo account to check out the kind of personal data they have. When we asked about the accuracy of the data and the possibility of manipulating it by sending messages to random numbers instead of the customer-defined category, the company said that after sending text messages to the target group, the company provides the customer with a report containing the numbers to which the messages were sent, but the numbers are incomplete, i.e., they are encrypted. The customer then selects some of these numbers, at which point, the company provides the full number, so the customer can contact the person to make sure that their data corresponds with the criteria selected.

The company Best 2 SMS gave us a quick offer by phone, explaining that its data is periodically updated and is obtained from several sources, including some municipalities, driver's license data, smart phone applications, the bar association's general directory and other sources. It is clear that the personal information of the Lebanese is up for sale by advertising companies, mobile operators, and others without any oversight.

● Car Registration Plate Numbers

In a report titled, "The Customs Rally: The Tax Evasion Race" produced by the investigative unit at Al-Jadeed TV, a number of senior Lebanese politicians, business owners, artists, and others were exposed for neglecting to pay their cars' customs duties. During their investigation, the reporters were able to obtain a list of names of Lebanese citizens and other residents who were granted a duty-free temporary admission for their cars, which allowed them to avoid paying any fees. This list was on CD-ROMs that held the personal data of all citizens and residents who own a car in Lebanon. Journalist Hussein Mehdy, an author of this study, worked with Al-Jadeed on this investigation and viewed the content of the CDS. The data is unencrypted and unprotected and was archived using Microsoft Excel and another rudimentary program.[44]

This infraction is not exceptional, however, since data associated to vehicles registered with the vehicle registration center is leaked on an annual basis. The leak, circulated on CDs, contains private and personal data such as the registered car owner's full name, along with their date and place of birth, registration number, place of residence, cell number, and home phone number.[45] The CDs are first obtained by intermediaries who then sell them to others.

Despite its repeated occurrence, the authorities have not taken any action to combat this data leak, which not only violates the privacy of citizens, but also jeopardizes their well-being and security. These CDs could fall into the hands of gangs specialized in car theft and can be used to forge the papers of stolen cars to sell them.[46] Beyond the financial consequences, this also poses a security risk. The leaked numbers of car registration plates could be used in terrorist operations and could enable the movement of wanted individuals, according to the head of the International Anti-Theft Bureau at the Judicial Police Unit, Colonel Fouad Khoury.[47]

Once public, this data has also been used on mobile apps, making the personal details of any driver accessible to virtually anyone, anywhere.[48] While apps such as Cars 961 are usually removed after complaints by citizens impacted by this breach, the data remains in circulation.

The Lebanese state began issuing biometric driver's licenses on January 4, 2017 by contracting with Inkript, the same company tasked with the issuance of biometric passports. However, according to Elie Nasr, as long as the Governing Body of Traffic has not adopted protection systems for information stored on computers belonging to the car registration centers, the data will remain unprotected.

Section 4: The "Electronic Transactions and Personal Data Protection" Draft Law

The first step toward developing personal data protection legislation dates back to 2005, when the first draft bill on Communications, Writing and Electronic Transactions was written. The draft was prepared at an earlier stage and launched under EcomLeb at the initiative of the Ministry of Economy and Trade and with the financial support of the EU. In August 2010, the advisory committee of the Lebanese parliament, headed by MP Ghinwa Jalloul, submitted a revised version of the EcomLeb bill, which drew negative reactions from civil society organizations and the legal community.[49] At the beginning of December 2011, MP Boutros Harb proposed a law on electronic transactions based on the same study.[50]

Currently, the "Electronic Transactions and Personal Data Protection" bill is being debated before a subcommittee formed by the joint parliamentary committees. Representatives from certain ministries such as the Ministry of Economy, the Interior and Communications, as well as a representatives from the Cybercrime and Intellectual Property Bureau, Banque du Liban, the Bar Association in addition to judges and academics are taking part in the discussions. In an interview conducted by SMEX with a number of lawyers from the Information and Communication Technology Center at the Beirut Bar Association, the Center described the bill as "a cross-breed, because it is the result of input submitted by several ministries and parties," adding however that "discussions will reduce these contradictions." In its participation in the debate, the Center is focused on adopting the law because there is an urgent need for it:

> *"People are now processing any and all data, which means that drafting a legislative framework will regulate this issue and put controls and sanctions in place. This way, rights and freedoms will be protected."*

In the beginning, members of the Information Center made a set of observations about the ongoing debate in the subcommittee. For example, the Center was surprised that the Ministry of Economy is in charge of receiving the data processing permits. It would make more sense for the Ministry of Communications to have that authority, especially since the security of personal data is related, in its broadest sense, to the internet and communications technology.

> *"Advisers from the various ministries would attend meetings mainly to make sure issues related to their ministries would pass without modification and to preserve powers for their respective ministries. For example, there was a power struggle between the ministries of economy and communications. In addition, Banque du Liban refused to discuss the issue of banking transactions, so the section on banking transactions was included in the law as proposed by the Central Bank without any discussion."*

For its part, the Information Center affirmed the Bar Association's own priorities regarding this law, namely, to protect and safeguard rights. The Center is trying to benefit from its participation in the discussions to reach the following goal:

> *"Every issue that raises our suspicion in terms of its content or effect prompts us to wage a battle to amend it. There has been a heated debate about the broad powers of the Public Prosecutor's Office with regard to blocking websites. In fact, the public prosecutor combines through their office three powers, namely, prosecution, investigation, and decision-making, which is contrary to the standards of justice and the right to a remedy. For example, the Cybercrime and Intellectual Property Bureau sends the public prosecutor a list of sites which they believe violate public morals or break certain laws. The public prosecutor then decides to block them and closes the case, making it impossible to even object or request a review."*

The Information Center does not believe there is a need for a specialized judicial body to protect personal data. In terms of prosecuting and investigating crimes related to this issue, it is better to establish a specialized public prosecution office. The Information Center explains that its efforts are mainly focused on Section V of the bill, dealing with the protection of personal data. In this context, the center points to a set of articles that they believe need to be amended. Therefore, the report will review the content of the five chapters of Section V, including the issues that are still under discussion.

• Section V on Personal Data Protection

Chapter I - General Provisions Concerning the Protection of Personal Data

The Bar Association has not registered any objection to the content of this chapter of the draft law. All automated and non-automated personal data processing are subject to its provisions, except for processing related to the exclusive activities performed by a person exclusively for that individual's needs. This chapter addresses the following principles and rights:

A. Law relating to public order: Chapter I of Section V stipulates that violations of the provisions listed in this section are unacceptable. Therefore, a data subject's decision to waive rights enshrined under this law has no legal value. The draft law enshrines the provisions contained therein as part of the public order, which means any violation of these provisions is subject to prosecution and nullification, regardless of whether or not the person whose rights are violated wants to proceed with the prosecution.

B. Right to know: The right to be informed is considered one of the basic guarantees to prevent abuse by any public person (public administration, municipality, public official, etc.) or private person (private company, institution, any ordinary person) in exercising their authority when processing an individual's personal data. According to Article 86 of the draft law, "Everyone has the right to know and to object before the data controller to the information and analysis used in automated processing pertaining to them and invoked against them."

Chapter 2 - Collection and Processing of Personal Information

This chapter does not include any provisions that the Bar Association finds objectionable. The bill provides for a number of necessary conditions for the protection of personal data during processing, and that includes having the data controller bear a central responsibility in this regard. The last article of chapter 2 (Article 93) stipulates that "all measures, depending on the nature of the data and the risks resulting from its processing, shall be taken to ensure its integrity and security and to prevent its distortion, damage, or access by unauthorized persons."

The conditions included in this section are as follows:
Safe and legitimate processing: "Collecting data of a personal nature with integrity and for legitimate, specific, and explicit objectives" (Article 87).

- Commitment to the specific objective of the data collection, provided that the objective is legitimate and clear: "The data shall be appropriate and not in excess of the stated objectives and shall be correct, complete, and properly updated" (Article 87).

- Commitment to the specified processing period: "The data can not be processed at a later time for purposes that are not in line with the stated goals, unless the data is being processed for statistical, historical, or scientific research purposes" (Article 87).

"The retention of personal data shall be lawful only during the period specified in the processing permit or in the decision authorizing it" (Article 90).

- Securing data on the health status, genetic identity and sexual life of individuals: "Collecting and processing personal data is prohibited if it reveals, directly or indirectly, the health status, genetic identity, or sexual life of a data subject."

Exemptions:
The article itself stipulates certain exemptions to these rules:

- When the data subject has made the data available to the public or explicitly approved its processing, unless there is a legal prohibition.

- When data collection and processing is necessary to make a medical diagnosis or provide medical treatment by a member of a health profession (The laws governing this profession impose confidentiality and punish any breach thereof).

- When vindicating a right, or defending it before the courts.

- In the case of obtaining a permit in accordance with the provisions of Article 97 of this law, the Minister of Public Health shall be the competent authority to grant such permit in accordance with said Article.

Chapter 3 - Procedures Required for Processing

A. Permit and Authorization

The difference between a permit and an authorization is fundamental. The first only obligates a person to inform the competent authorities of the activity they wish to perform in accordance with the law and within its provisions. Therefore, it is just a notification and is not subject to the authorities' acceptance, or rejection. In contrast, the authorities may grant an authorization to an applicant or refuse it, after ascertaining the conditions that must be met to have such an authorization.

The first article of this chapter (Article 94) specifies the entities allowed to process data without having to obtain a permit first. The Bar Association argues that two additional categories of processing must be exempted from having to obtain a permit: data processing carried out by persons of the public right, each within the framework of their mandate, and the transactions provided for in the Telecommunication Interception Act, which regulates the mechanisms used for intercepting telephone calls.

The Telecommunication Interception Act (Law No.140/1999) regulates the mechanisms for obtaining an authorization to intercept and monitor communications. The Ministry of Communications is the competent authority to grant this kind of authorization. Adding this category is therefore necessary to protect the data processed following the interception of a call. It also prevents a conflict of mandates between the Ministry of Telecommunications (authorized under the Telecommunication Interception Act to grant authorizations to intercept calls) and the Ministry of Economy (given general jurisdiction to grant authorizations under the Electronic Transactions and Personal Data Protection draft law). Such a conflict of mandates could open the door to violations of people's data under a legal cover.

It seems self-evident that persons of the public right — meaning all administrations and institutions of the Lebanese state, both central and local (ministries and municipalities) — would be exempt from having to get a permit. It is unreasonable to ask the state to grant itself a permit through one of its ministries to process data belonging to its citizens or those residing on its soil. The priority should be to include in the law itself the greatest possible guarantees for the rights of individuals, in particular, their right to appeal and to seek redress before the courts if the privacy of their data is violated and to incorporate all the necessary safeguards to ensure that persons of the public right do not abuse their privileges vis a vis individual citizens.

The permit therefore should be the general rule in the bill, meaning, processing in general should be done with a permit, but some data will need an authorization for processing. These fall into three categories:
1. Data related to the state's internal and external security requiring a joint decision by the Ministers of National Defense, the Interior, and Municipalities
2. Data related to criminal offenses and judicial proceedings requiring a decision by the Minister of Justice
3. Data related to people's health status, genetic identity, and sexuality requiring a decision by the Minister of Public Health.

B. Deadline for Issuing an Authorization

The article, as currently drafted, does not provide a specific deadline for granting or denying an authorization. The Bar Association argues that the decision by the aforementioned parties must be linked to a clear deadline so that this article does not become an opportunity to prevent the processing of data by legal means and within the guarantees provided for by law. This will lead to a return to unorganized processing of personal data. Therefore, the Bar Association proposes adding a clause specifying a clear deadline for issuing the authorization decision (two months after submitting the application), whereas the silence of the competent authority after the expiration of the deadline shall be interpreted as an "implicit approval."

C. Authority Tasked with Receiving Permit Requests

This chapter names the Ministry of Economy and Trade as the ministry in charge of receiving requests for data processing permits, and details the data to be included in the permit (Article 96). The Ministry of Economy and Trade has a duty to the public to publish a set of information about the data collector (Article 98).

Chapter 4 - Right of Access and Correction

It is remarkable that a full chapter has been devoted to this right, which reflects the great importance it is given, at least in principle. Access to data, i.e., the data subject's access to data collected about them and is subject to processing, also known as the right to know, is a fundamental guarantee for the protection of data from any violation or excessive collecting, processing, or use for a reason other than what it is intended for. The same goes for the right of correction. It protects people from the transmission and dissemination of erroneous data about them or its processing in any way.

The significance of this chapter has made it the subject of discussions and disagreements. The Bar Association proposed amendments to all its articles. This chapter includes the right of the data subject to obtain data, request its correction, update, or deletion, and the right to resort to "the competent judicial authority, specifically, a summary judge." It also includes the rights of the data processor, such as requesting financial compensation for carrying out the processing or rejecting applications of an improper character.

The Bar Association's criticism was limited to the characterization of the person who enjoys this right. While the current text of the draft law grants "every interested person" the right to access and rectify data, the association insists that this term, wherever it is mentioned in the chapter, should be replaced with the more exclusive term "the data subject or any of their heirs," in order to guarantee individuals their right to privacy.
The Bar Association also proposes removing the phrase: "The heirs of an interested natural person may ask the data controller to introduce new modifications after the death of the inherited person," simply because it is impossible for the dead person to object to any wrong information that might be listed about them if the data is allowed to be modified after their death, which should necessarily lead to suspending any modification to the data (Article 101).

The Association also proposes amending Article 99, regarding the content of the personal data that the data subject or their heirs may request from the data controller. The bill allows "every interested person" to request, for example, "information about the recipients of personal data or those who can access the data." This article makes it possible to have access to the data of a large group of individuals out of curiosity. This means legalizing infringement on the privacy of others. Therefore, the Bar Association proposes amending this clause to read as follows: "The person who is the subject of personal data or any of their heirs may also request from the data controller, in accordance with the conditions specified in the second paragraph above, handing over the following additional information: The purpose of processing, the categories, the source, the subject of processing, its nature, the recipients of the personal data and those who can access it, the categories, the timing, and the purpose of such access."

Chapter 5 - Penal Provisions

The penalties provided for in this chapter for breaching the confidentiality of data outside the legal framework, range between a fine of 15,000,000 Lebanese pounds (9,957 USD) and a 3-year prison sentence. The only amendment proposed to this chapter by the Bar Association, is determining the time limit after which the data controller's refusal to process personal data becomes a misdemeanor. This time limit, according to the association's proposal, must be 10 days. If, after this period, the data processor refuses to respond to the person making the request, the processor's behavior shall be considered a misdemeanor punishable by a penalty ranging between 1,000,000 and 15,000,000 Lebanese pounds (664 USD - 9,957 USD).

- **Evaluation of the Draft Law in Light of ESCWA Directives**

Within the framework of the project Regional Harmonization of Cyber Legislation to Promote the Knowledge Society in the Arab World, ESCWA has developed a list of directives on cybersecurity. These directives are the result of an in-depth review of a wide range of legislations, conventions, and studies in this area, including international conventions, directives and recommendations issued by the EU, resolutions issued by the UN Council, the Council of Europe and the International Telecommunication Union (ITU), in addition to a number of Arab and international legislations.[51]

Comparing the Lebanese draft law to the ESCWA directives issued in Beirut shows a discrepancy between the guarantees needed to protect people's data based on the directives and those stipulated in the draft law. The similarities between the directives and the draft law are the following:

- The right to know
- Secure processing
- Commitment to a specific period for processing
- Notification and transparency obligations towards the data subject
- The right to access and rectify
- Permit and authorization: Linking the possibility of processing to submitting a permit to a competent authority, provided that processing based on a permit is the general rule, except for a set of data determined by the state, whose processing requires obtaining an authorization
- Guarantees for not relying on machine-processed data to take any administrative or judicial decisions vis a vis the data subject
- Prohibiting the processing of data related to health status, genetic identity and sexuality

However, the segment on prohibitions is brief in the text of the Lebanese draft law, whereas the ESCWA directives provide for "the prohibition of processing personal data that reveal racial or ethnic origin, political, religious or philosophical views, and trade union affiliation in addition to the data related to a person's health status and sexual life."

Both the ESCWA directives and the Lebanese draft law contain exceptions to the prohibitions. Theoretically, it might appear that there are less exceptions in the Lebanese draft law, thus enabling a broader application of the prohibitions. Practically, however, one should caution against the exception that allows data processing based on an authorization issued by the Minister of Public Health (in accordance with article 97). This exception constitutes an opening to expand the limits of the prohibition to the point of eliminating it. In contrast, the ESCWA directives are devoid of this exception.

- **Principles outlined in the ESCWA directives**

Contrary to the ESCWA directives, the draft law does not enumerate cases where the processing of personal data is permitted. There is a tendency in the Lebanese draft law to consider data processing as originally free and unrestrained, requiring only submitting a permit to the Ministry of Economy, except for specific cases that require an authorization. On the other hand, the ESCWA directives assert that processing personal data can not be subject to the principle of "freedom is the origin;" it must be restricted because it is related to the personal lives of others. The directives therefore stipulate that "personal data can only be collected in the following cases: either for data subjects to give their consent, to implement a contract in which data processing is necessary, to ensure commitment to a law by a data controller, to preserve a vital interest of a data subject, to implement a task related to the public interest to play a part in exercising public authority on behalf of the data controller or the data recipient, or to achieve the legitimate interest of the data controller or the data recipient."

- **Transfer of personal data to foreign countries**

The Lebanese draft law is devoid of any mention of the principle that it is not permissible to transfer personal data that is being processed to a foreign country. The ESCWA directives have enshrined this principle, making it dependent on the requirement that the foreign country provide an adequate level of legal protection, whereby data transfer becomes possible. There are many concerns about the omission of this clause in the Lebanese draft law, especially as Lebanon is a country of refuge for many people fleeing dictatorships, conflicts, and wars. This is especially concerning because Lebanon is bound by agreements compelling it to provide personal data about individuals to their countries of origin. For example, Lebanon is a member of the Arab Convention for the Suppression of Terrorism. According to this convention, each signatory state commits to provide any other signatory state with information or data that would contribute to the fight against terrorism. Included in the data that could be exchanged is "the description of a wanted person with the utmost possible accuracy and any other data that might identify them, their nationality, and identity." While the goal behind this convention might be noble in principle, the arbitrary application of terrorism laws and their use in violating human rights in many Arab countries lead to the conclusion that this convention opens the door widely for violating the data of every resident of Lebanon and endangering their lives in their countries of origin, as long as the Lebanese legislation lacks any regulation protecting personal data.

- **Monitoring Body**

The first draft of the Electronic Transactions and Personal Data Protection bill included provisions

establishing an independent body to monitor its implementation and compliance with its provisions; however, these articles have been removed and the current draft does not contain any mention of a similar body. The ESCWA directives on the other hand, include an article stipulating the need for cyber laws to establish a "specialized official oversight entity."Its function is primarily to monitor the proper implementation of the directives and it should be able to exercise its functions independently.

The powers of this body include:

- Receiving personal data processing permits and issuing authorizations
- The right to investigate, including having access to data and collecting information in order to carry out its monitoring role
- Intervening and imposing administrative sanctions, such as preventing data processing or preventing access, deletion, or destruction of data
- Appearing before the courts if the directives are violated
- Providing advice and suggestions to develop legal texts
- Cooperating with foreign bodies specializing in the area of personal data

Conclusion

In its current form, the "Electronic Transactions and Personal Data Protection" draft law has many weaknesses that render it practically useless, despite the parliamentary committees' lengthy discussions on the proposed legislation.

Even though its rules are of a commanding nature and not limited to automatic and digital processing of data, its many exceptions narrow the margin of protection for personal data (articles 87, 91, 92, 94, 103, for instance). The draft states that the ministry mandated to issue licenses and receive authorizations to collect and process data is the Ministry of Economy and Commerce, the executive authority. This is another point of weakness because the judicial authority should be tasked with monitoring and respecting private life and public freedoms, as opposed to the executive branch.

Reconciling between the principle of freedom and the need for security, and finding the right balance between the right to access information and the right to protect privacy and personal data is only possible through the creation of an independent administrative body. If this is not feasible, the task can be handed over temporarily to the conflict resolution committee that was announced in Law 659, issued on February 4, 2005.

Prior to the creation of such a body, the legislature should amend Article 97 (related to the formation of the committee), amend Article 98 (related to the competencies of the committee) in order to require adherence to the principle and rules of Bill 934. After its formation, this body should have the authority to issue licenses and receive authorizations to process data.

Bibliography

[1] SMEX. (December 14, 2016). Mapping the Landscape of Digital Surveillance in Lebanon. https://www.smex.org/wp-content/uploads/2016/12/SMEX-Landscape-Mapping-of-Digital-Surveillance-in-Lebanon.pdf

[2] SMEX. (December 16, 2016). Call for Applications: The SMEX Fellowship for Reporting on Digital Freedoms. https://smex.org/call-for-applications-the-smex-fellowship-for-reporting-on-digital-freedoms/

[3] Law No. 140 was issued at a time when the means of intercepting the privacy of individuals and their personal data were not regulated or subject to any legal provisions. The constitutionally-mandated protection was virtually non-existent and any person was susceptible to having their privacy and personal data violated. This law was informed by the letter and spirit of French law No. 646/1991. However, failure to issue regulatory decrees to implement the law as quickly as possible and the failure of the independent body, tasked with verifying the legality of administrative interception of phone calls, to do its job prior to 2011 undermined the effectiveness of the law as SMEX will demonstrate in this study.

[4] Article 2, loi n 2004-801 du 6 août 2004: Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.

[5] UNESCWA. (2012). ESCWA cyber legislation directives, Project for Regional Harmonization of Cyber Legislation to Promote the Knowledge Society in the Arab world. https://www.unescwa.org/sites/www.unescwa.org/files/page_attachments/directives-full.pdf

[6] The definition according to the French law:
Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction

[7] Barjas, E. (2017). "Eleven years after its establishment, the Dispute Settlement Committee began its work." The Legal Agenda, (48). http://www.legal-agenda.com/article.02_php?id=36

[8] Law No. 140/1999.

[9] Law No. 431/2002, Article 38.

[10] Privacy International. (March 2015). A report on the Right to Privacy in Lebanon prepared by SMEX, Privacy International (PI) and the Association for Progressive Communications (APC) during the 2016 Universal Periodic Review (UPR). https://www.privacyinternational.org/sites/default/files/Lebanon_UPR_23rd_session_Joint_Stakeholder_submission.pdf

[11] The Arab Center for Legal and Judicial Research, the Arab League - The Council of the Arab Ministers of Justice. (August, 2016). The Second Conference of Specialists on Cyberspace Security and Safety (Internet). http://bit.ly/2wtKt14

[12] The Arab Convention for the Suppression of Terrorism signed in Cairo on April 22, 1998. Lebanon joins the Convention. The Authorization to Ratify, and content of the Convention. (April 22, 1998). http://www.madcour.com/LawsDocuments/LDOC-44-635278203054882024.pdf

[13] Rammal, S. (2016) "The Right to Privacy in the Digital Age (An Analytical Reading in Light of the General Assembly Resolution 68/167)."

[14] Rouse, M. (2015, November). O-code/low-code app development evolves from loathed to loved, Essential Guide, biometrics. http://searchsecurity.techtarget.com/definition/biometrics

[15-16-17-18] Information Commissioner RS. (2008, February). Guidelines for the introduction of biometric measures. https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Guidelines_Biometrics.pdf

[19] No-code/low-code app development evolves from loathed to loved. http://searchsecurity.techtarget.com/definition/encryption

[20] Elie Nasr is an expert in information security and chair of the Department of Information and Communications Technology at the American University of Science and Technology (AUST).

[21] A statement by the Lebanese Directorate of General Security. (2017) http://www.general-security.gov.lb/ar/posts/221

[22] The Lebanese Directorate of General Security. (2014). The Smart Biometric Residence Permit. http://www.general-security.gov.lb/ar/posts/60

[23] The Lebanese Directorate of General Security. (2016). Issuing Lebanese Biometric Passports. http://www.general-security.gov.lb/ar/posts/182

[24] Letter from the Directorate of General Security to SMEX on May 26, 2017

[25] Shoufi, E. (January 8, 2016). "Passport Renewals: Fees Paid Twice," Al-Akhbar newspaper. http://www.al-akhbar.com/node/249438

[26] Shoufi, E. (January 9, 2016). "200,000 Passports Go 'Obsolete'," Al-Akhbar newspaper. http://www.al-akhbar.com/node/249546

[27] Mounzer, R. (January 9, 2016). "The General Security Clarifies the Question of Passport Replacement" al-Joumhouria newspaper. http://www.aljoumhouria.com/news/index/283847

[28-29] Akil, R. (2016). "The Passport... with Full Confidence," The General Security Magazine (29). http://www.general-security.gov.lb/ar/magazines/magazine/42

[30] Ballout, M. (June 20, 2016). "This is the Story of the Biometric Passport... and the Mechanism of the Billion Dollar Grant." Assafir newspaper. http://assafir.com/Article/426382

[31] The Gemalto website

[32] The Inkript website

[33] Neal, D. (February 25, 2015). "Gemalto: It looks like we were hacked by GCHQ and NSA." https://www.theinquirer.net/inquirer/news/2396223/sim-card-security-scare-gemalto-is-investigatiing-uk-and-us-hack-allegations

[34-35] ISO/IEC 19794-7:2014 . (2014). https://www.iso.org/standard/55938.html

[36-37-38] Al-Dirani, Z. (May 28, 2013). "The AUB Administration Spies on its Population." Al-Akhbar. http://www.al-akhbar.com/node/183870

[39] AUB Leaks. (n.d.). https://aubleaks.wordpress.com/

[40] B Mehdy, H. (December 9, 2014). "Judicial Precedent in the AUB leaks Case: Consecrating the Principle of the Precedence of Public Interest." al-Akhbar newspaper. http://al-akhbar.com/node/221518

[41] Hawi, Z. (February 4, 2016). "Hussein Mehdi the 'leaker' Goes before a Judge. al-Akhbar newspaper. http://www.al-akhbar.com/node/251352

[42] Alfa Website. (n.d.). Description of service. Alfa Media. Retrieved from https://www.alfa.com.lb/media/sms.aspx?language=1&cat=1&subcat=1

[43] Touch website. (n.d.). SMS Advertising. Mobile Media. Retrieved from https://www.touch.com.lb/autoforms/portal/touch/business/sms-advertising/mobile-media

[44] "The Customs Rally: The Tax Evasion Race." Riad Kobaissi. (2017). https://www.youtube.com/watch?v=DLgu0v4RaN4

[45] Sada Saida. (March 14, 2013) "A Disaster in Lebanon... Violations and Attacks." http://www.sadasaida.com/news.php?go=fullnews&newsid=29853

[46-47] Mokaddam, N. (February 23, 2010). "Forging Car Registration Plates: Gangs benefiting from the Vehicle Registration Center. http://al-akhbar.com/node/58400

[48] Tanios, C. (February 25, 2015). "A New Scandal: Your car registration plate now exposes the details of your life!" Annahar newspaper.http://bit.ly/2upL71S

[49] Makhlouf, Y. (September 26, 2011). "The Electronic Transactions Regulation Draft Law: Distinction in declaring the principle of "respect for privacy" and distinction in destroying it. The Legal Agenda. http://www.legal-agenda.com/article.php?id=31

[50] The official website of the Lebanese parliament. (December 1, 2011). Parliamentary Activities. https://goo.gl/HrC1Qn

[51] ESCWA Cyber Legislation Directives, issued in Beirut 2012.

Authors' Biographies

Elham Barjas is a journalist and legal researcher who documents and reports on judicial processes and legal procedures with the goal of advancing human rights in Lebanon. Elham is currently also writing her master's thesis on constitutional law. Her work has been featured on Al-Modon, Al-Deyar, and Al-Akhbar among others.

Hussein Mehdy is a journalist with experience in print, broadcast, and digital media.
Hussein has exposed corruption and fraud at several prominent Lebanese universities, including the American University of Beirut and the Lebanese University.

Sara Rammal holds a Master's Degree in Public Law from the Lebanese University (LU) and a Diploma in International Law from Adam Mickiewicz University (AMU) in Poznan, Poland. She is the author of "Right to Privacy in the Digital Age: Analytical Reading in light of the UN General Assembly Resolution 68/167."

Dr. Pierre Al Khoury is a legal expert in the fields of information and communication technology (ICT) and consumer protection. He teaches commercial, contracts, corporate, and ICT law. He is also a lawyer and a member of the Bar Association, specialized in intellectual property and ICT laws. He is the legal head of Creative Commons in Lebanon and a member of the parliamentary subcommittee currently studying the electronic transactions and personal data bill in the parliament.

SMEX