Law No. 81 Relating to Electronic Transactions and Personal Data

The President of the Republic publishes the following law as passed by the Chamber of Deputies:

Single Document

- The draft law issued by decree no.9341 of November 17, 2012 was ratified as amended by the joint parliamentary committees and the parliament.

- This law shall be published in the Official Gazette and shall enter into effect within three (3) months of its publication date.

Baabda, on October 10, 2018

Signature: Michel Aoun

Issued by:

The President of the Republic

The President of the Council of Ministers

Signature: Saadeddine Hariri

President of the Council of Ministers

Signature: Saadeddine Hariri

<<<<>>>>

The Electronic Transactions and Personal Data Law

Preamble

Article One:

For the purposes of the present law, the below terms will have the meaning assigned to them as follows:

Writing: The process of writing or recording letters, numbers, characters or symbols, provided that they are legible and comprehensible, regardless of the format used (paper or electronic) and the medium through which the information is transferred.

Electronic Document: An ordinary or official document as defined by the Civil Procedure Law, issued in an electronic form pursuant to Article 8 herein.

Signature: The signature required to complete a legal process in order to identify the party thereto and confirm their consent to the signed legal process.

Service Provider: A public or private law enforcement officer who issues the certificates of authentication after applying the protection measures to secure one or all of the functions outlined in Article 15 herein.

Electronic Commerce: An activity whereby a person provides or remotely offers goods and services to another person.

Bank Card: An instrument issued by a bank or an institution licensed by Banque Du Liban, allowing its holder to withdraw cash money or perform electronic payments or any other banking or financial services.

Electronic Money: Electronic monetary units stored in electronic form.

Network Service Provider: A business or organization that enables the user to access an electronic communication network and provides the latter with direct information transfer services, including the temporary storage of information sent provided it does not result in the modification of any stored data and the storage of information is solely used to deliver the service successfully without exceeding the assigned time limit.

Data Host: A system used to store third-party information of any type, either free of charge or in return for a consideration, and make it accessible to the public through direct communication services.

Traffic Data: Any data relating to a communication by means of a computer connected to the network, generated by a computer system and indicating the communication's origin, destination, route, format, intent, time, date, size, duration, etc.

Domain Name: The system used to translate the alphanumeric domain name of a website into an Internet Protocol number.

Personal Data: Any information that helps to directly or indirectly identify a natural person, by comparing the data or overlapping data collected from multiple sources.

Processing of Personal Data: Any action or set of actions performed on the data regardless of the medium used, including data collection, recording, organization, storage, adaptation, modification, extraction, reading, use, transmission, copy, dissemination, deletion, destruction or otherwise disposing of it.

Personal Data Subject: The natural person which the data enable to identify.

Personal Data Processor: The natural or legal person responsible for setting the processing objectives and methods.

Personal Data Recipient: The person authorized to receive the personal data and he should be different than the personal data processor. The public authorities which have a legal mandate to request personal data are not considered as personal data recipients.

Article 2:

The information technology is at the service of the people, provided that it does not prejudice their individual identity, rights, private life, or individual or public freedoms.

Article 3:

The provisions of the applicable laws shall be enforced in all matters not mentioned in the present law and to the extent that they are not contradictory to its provisions.

Part I: Electronic Writing and Evidence

Chapter I: General Provisions

Article 4:

Electronic writings and signatures shall have the same legal effect as the writings and signatures made on paper or any other medium, provided that the person producing them is identifiable and that they are organized and stored in a way that preserves their safety. Any electronic writing that does not meet the criteria above shall be considered as introduction of written evidence.

Article 5:

The expression "storage of electronic data" mentioned in Article 4 above means the recording of the data on a storage medium in a way to ensure that the data is safe and accessible at all times in a way that allows copying or extracting content.

Article 6:

The electronic documents shall be governed by the Civil Procedure Law and other applicable laws as deemed appropriate according to their electronic nature and the general provisions stipulated herein.

Trade books are governed by the relevant provisions in the Code of Land Trade.

Chapter II: Electronic Documents as Evidence

Article 7:

The electronic document shall be accepted as evidence and is deemed to have the same significance and power of proof as the written paper-based document, provided that it is possible to identify the person issuing the document and that the latter is organized and stored in a way that ensures its integrity.

Article 8:

Official electronic documents do not produce any legal effects unless they are organized and governed by virtue of a decree issued by the Council of Ministers upon a proposal by the Minister of Justice.

Said decree shall govern the special procedures and guarantees pertaining to the documents and their scope.

Article 9:

The electronic signature is issued through the use of a safe medium that identifies the signatory and provides a guarantee that the signature corresponds to the legal process in question.

If the signature is linked to the protection measures authenticated by the authorized authentication service provider according to Chapter Four herein, it shall be presumed to have satisfied the criteria set forth in the subsection (1) of the present Article, unless proven otherwise.

Article 10:

The multiple copy rule stipulated in Article 152 of the Civil Procedure Law is deemed satisfied when the ordinary document is organized as per the reliability requirements herein, and when each party's mechanism allows to obtain or access a copy of the document.

Article 11:

When the law does not stipulate other rules and when the parties fail to conclude an agreement to this effect, the judge shall arbitrate the disputes arising from the written evidence in case of multiple documents, and determine through all possible means the most reliable document regardless of the medium, while taking into consideration the official document's power of proof.

Article 12:

When denial, or refusal to acknowledge, or claim of forgery are not related to an electronic document or electronic evidence, the judge shall, when conducting an investigation as per the provisions of the Civil Procedure Law, ensure that all the reliability requirements to confirm the validity of the electronic document or signature are met. In other terms, the judge shall ensure that the document was organized and stored in conditions that preserve its integrity, and that the person issuing the document can be identified through a reliable mechanism as per Articles (7) and (9) herein.

The judge may request the parties to provide all the digital traces in their possession, or appoint an expert to look for such traces or resort to technical expertise.

In all circumstances, the general rules pertaining to denying signature or claiming forgery of electronic documents and signatures shall apply, depending on the nature of those documents and signatures.

Article 13:

An electronic document not meeting all the requirements set for in Articles (7), (9) and (10) herein may be considered as an introduction of written evidence.

Chapter III: Protection of Electronic Writings

Article 14:

Electronic writing is a free act, and no person shall be bound to resort to protection means unless otherwise stipulated by the law.

Article 15:

The protection measures are used in electronic writings and signatures to make them more reliable.

The protection measures help perform several functions, such as verifying the identity of the document organizer, assigning a correct date to the document, and/or ensuring its storage and the integrity of its content.

Any and all functions above are provided by one or more authentication service provider who shall, upon performance of said functions, deliver a certificate of authentication to the concerned person.

Any and all functions above may be performed through other techniques as well.

Article 16:

Pursuant to Article (133) herein, the provision of authentication services shall not be subject to pre-licensing. However, it is possible, at the request of the qualified authentication service provider and according to the provisions of Chapter Four under this Part, to obtain an accredited certificate issued by The Lebanese Accreditation Council ("COLIBAC") established by the Law No.572/2004 (notwithstanding Articles (4) and (11) thereof).

Article 17:

When the electronic signature is produced and authenticated through a procedure by an authorized authentication service provider, it is presumed to be reliable and to have satisfied the requirements set forth in Article (9) herein, unless proven otherwise.

Article 18:

If the electronic signature is produced or the electronic writing is organized, dated or stored through a authentication procedure provided by an unauthorized authentication service provider, the judge may, at their own discretion, assess the power of proof of the electronic signature or writing, unless the parties agree otherwise.

Article 19:

Both authorized and unauthorized authentication service providers shall be subject to the professional secrecy clause regarding the data requiring authentication, except for the information contained in the issued certificate.

The professional secrecy may be lifted if need be by virtue of a decision issued by the competent judicial authority to for the purpose of legal proceedings or arbitration.

Chapter IV: Accreditation Principles

Article 20:

COLIBAC accredits those authentication service providers who issue certificates to electronic writings and signature provided they meet the requirements outlined in Articles (7) and (9) above.

COLIBAC decisions regarding the implementation of the present Law may be challenged before the State Council.

Article 21:

COLIBAC shall develop the Terms of Reference (TOR) setting out the terms and obligations applied in the protection procedures proposed by the authentication service provider requesting accreditation. The Terms of Reference also identify the administrative, technical and financial components that should be enclosed with the accreditation application.

In order to identify the TOR technical specifications, COLIBAC takes into consideration the international standards and criteria for the electronic signature and other related products, services or software.

COLIBAC shall review the Terms of Reference at least once per year and as required in light of future technology developments.

Article 22:

For the purpose of issuing or renewing the accredited certificate, COLIBAC shall take into consideration the following criteria:

1- The infrastructure and technical measures undertaken to protect the electronic writing, the organizational procedures and the human resources delegated by the authentication service provider, all of which must be compliant with the international standards.

2- The audit periodicity and scope to ensure that the services provided by the authentication service provider are consistent with the latter's announcements and policies.

3- The presence of financial guarantees for the service provider to conducts their business.

4- The presence of an insurance policy against the financial effects of civil liability.

5- The guarantees of impartiality, independence and integrity by the authentication service provider.

6- The accreditation or previous assessment by a competent body of the quality of protection measures against international standards, if the authentication service provider is based abroad.

The above standards are used as well to assess the reliability of the protection measures provided by an unauthorized authentication service provider.

Article 23:

COLIBAC shall examine the accreditation application at the expenses of the authentication service provider requesting the accreditation. For this purpose, COLIBAC may request additional information from the service provider, including a request to conduct an investigation in the premises and with the employees of the service provider.

The examination process aims to verify that the TOR specifications are compliant with accreditation requirements, especially those protection measures they are seeking accreditation for.

Upon the completion of the examination process, COLIBAC drafts and sends its report to the authentication service provider for the latter to comment on it.

Article 24:

In light of the evaluation report and the authentication service provider's comments (if applicable), COLIBAC shall take its decision within no more than two months based on the requirements satisfaction (or lack thereof) by the provider.

In the event the time limit set out in subsection (1) elapses before COLIBAC has reached a decision, the application shall be automatically deemed rejected.

If COLIBAC decides that the authentication service provider satisfies the requirements, COLIBAC shall issue an accredited certificate outlining the protection measures encompassed by the accreditation, and shall determine its validity provided it does not exceed three years.

Article 25:

At any time during the accreditation period, COLIBAC may conduct an audit and may suspend or immediately revoke the accredited certificate in case of violation of the accreditation requirements, the Terms of Reference or the legally defined technical, administrative and financial components.

The decision to suspend or revoke the certificate may only be taken after allowing the provider's representative to express their comments within a time limit determined by COLIBAC.

Article 26:

The authorized authentication service provider shall notify COLIBAC in writing, through registered letter of any change that may affect the components proposed in the accreditation application, under penalty of enforcing Article (25) of the present Law.

Article 27:

The authorized authentication service provider shall deliver a copy of the certificate issued by COLIBAC to all parties requesting it.

COLIBAC shall publish and make accessible to the public a list of the accredited authentication service providers that is regularly updated, especially on COLIBAC website.

Article 28:

A authentication service provider based outside the Lebanese territories and satisfying the requirements may apply for an accreditation by COLIBAC.

Article 29:

Notwithstanding any agreement to the contrary, a authentication service provider is deemed responsible for the reliability of the protection measures covered in the accredited certificate and shall be bound to indemnify their clients for any damages resulting from the defective performance of his obligations under the contract.

PART II: Electronic Commerce and Contracts

Chapter I: General Provisions

Article 30:

Electronic commerce shall be free to the extent permissible by law.

All matters related to e-commerce and not mentioned in the present law shall be governed by the applicable laws, particularly the Code of Commerce, the Code of Obligations and Contracts, the Civil Procedure Law and the Consumer Protection Law.

Article 31:

All persons practicing e-commerce as a business must ensure to the persons they deal with an easy and direct access to the following information at all times:

1- For natural persons, their first name, last name and place of residence.

2- For legal entities, their name, the name of their legal representative, their headquarters and their commercial address.

3- The detailed address of the person's place of residence, their email, their website, their telephone number(s) and any other means of contact.

4- Number and Place of registration at the Commercial Registry and the competent tax department.

5- Their professional capacity and the professional rules or principles that govern their business, in case they were members of an organized profession or trade union.

6- A detailed statement outlining the price and any payable tax, fee or expenses.

Article 32:

Promotional ads that are accessible online through any electronic device should contain a reference to indicate that the material is a promotional ad and define the person for whom the ad was placed.

It is forbidden to communicate unsolicited marketing and advertising emails (SPAM) using a real person's name and address, unless that person has consented to such type of advertising, except for cases where the sender of the unsolicited advertisement has legally obtained the client's address through a previous engagement with them.

Every promotional or marketing email should contain a reference to an email which the recipient can reply to in order to request that they stop receiving such emails permanently and free of charge.

Chapter II: Electronic Commerce Contracts

Article 33:

Any person who offers, as part of their business, goods or services by electronic means shall include the following in their offerings:

1- Steps to follow to sign the contract electronically.
2- The contract terms and conditions in a form that can be saved and duplicated.
3- Technical features that allow the addressee to double check the electronic contract for errors and correct the same before submitting the final approval to conclude the contract.
4- To which extent the offeror undertakes to store the digital traces of the negotiation and the contract signed. In case of such undertaking, the offeror shall determine the duration thereof, the method by which they will store the digital traces, and the conditions for accessing the stored documents.
5- The contract official language.

Article 34:

The offer shall be binding to the offeror for as long as it can be accessed by electronic means.

Article 35:

The offeror shall notify the other party of receiving their consent within a reasonable time limit or within the time limit specified in the offer.

The offeror shall indemnify the other party for any damage resulting from a breach of this obligation.

Article 36:

Articles (33) and (35) of this Law shall not apply to contracts that are exclusively concluded through exchange of emails or through separate personal correspondences.

Article 37:

In contracts signed between dealers alone or professionals alone in e-commerce, or between dealers and professionals, the parties to the contract may choose not to abide by the provisions of Articles (33) and (35) above.

Article 38:

The acceptance of the electronic means to be used in civil or commercial contracts shall not be considered sufficient to originate the contract. The addressee may re-examine the parties' contractual obligations before confirming their will to proceed with the contract.

When bargains in civil and commercial contracts are made electronically, the contract shall only be originated when the offeror receives the addressee's consent.

An electronic communication is taken to be dispatched when it enters the first information system outside the sender's control.

An electronic communication is taken to be received by the addressee in the following cases:

1- When it enters the system designated for receipt by the addressee.
2- When the addressee extracts the electronic communication from a private electronic address, in case no specific information system is designated for receipt.

Unless proven otherwise, an electronic communication is taken to be dispatched from the sender's place of business and received at the addressee's place of business. If the offeror or addressee has more than one place of business, the one with the closest relationship with the underlying transaction is considered. If there is no such transaction, the principal place of business is considered. If the offeror or addressee has no place of business, the legal domicile or ordinary place of residence is considered.

The offeror and the addressee may agree on special rules that govern sending and receiving electronic communications.

Article 39:

If civil and commercial contracts require organizing a written document for the contract to be legally valid, such document may be written and saved in electronic form if both the document and signature satisfy the rules of evidence, as specified in Articles (7) and (9) above.

If a contracting party must include any handwritten statement, they may do so in electronic form if it guarantees that the statement may only be originated by said contracting party.

Article 40:

The competent interim relief judge is entitled to require compliance with the obligations set forth in Articles (31) and (32) herein under penalty of coercive fine.

The subject matter jurisdiction of the interim relief judge does not preclude filing a counterclaim for damages before civil courts or bring legal action in competent criminal courts.

Article 40 bis:

The provisions of the Consumer Protection Law shall apply to matters related to electronic commerce provided they do not conflict with the present Law.

Chapter III:
Electronic Banking and Financial Services

Part I: Electronic Payment and Money Transfer

Article 41:

An electronic payment or money transfer is an operation carried out, partly or entirely, by electronic means. In order to perform such operation, the client authorizes the bank, the financial institution or any institution legally authorized or licensed by *Banque du Liban* to perform an electronic payment operation, electronic money transfer or credit push/debit pull payments through their account or another account.

The expression "electronic means" is subsection (1) refers to any and all electronic means, including digital means, provided by one of the aforementioned institutions or subsidiary thereof, and used by the client to perform or instruct to perform one or several electronic payments or money transfers.

Article 42:

When the institutions, referred to in Article (41) herein perform electronic payments or money transfers, they shall make sure that such transactions comply with the applicable laws and Banque Du Liban regulations.

Article 43:

The client shall give his prior written consent to the conditions governing electronic payments, transfers or cancellation thereof, provided that such conditions are clear, explicit and compliant with Banque du Liban regulations, include the rights and obligations relating to electronic banking services and determine the fees, expenses, commissions and taxes, if any.

Article 44:

The institutions stated in Article (41) herein shall notify the client, in writing, at least 30 days prior to any amendment to the contract conditions.

The client either consents to such amendments or terminates the contract with the said institutions.

However, in justified exceptional cases, such as the case where the standards of protection, safety and preserving the integrity of the client's account or of the electronic payment/transfer system should be met, the institutions referred to in Article (41) herein may set restrictions on electronic payments and transfers performed by the client, provided that they promptly communicate such restrictions to the client who bears no financial liability as a result.

Article 45:

The electronic means used shall be able to communicate and store the electronic payment or money transfer order, thus allowing clients and institutions to refer thereto where appropriate.

Institutions referred to in Article (41) above shall use a technical system to identify the entity issuing the order to perform an e-payment or transfer, and to prove that the client has indeed made such order to the institution.

Said institutions shall also use an information system that promptly informs the party giving the order, in writing, whether the order was accepted or rejected, and the causes of rejection.

In case the rejection was due to a material error, there should be a possible process in place to fix it. To this effect, Banque du Liban shall be solely responsible for specifying the basic standards of said system.

Article 46:

Except in cases of serious error, gross negligence or bad faith, the client shall not be responsible for any electronic payment or transfer transaction made to their account provided that they promptly notify in writing the institutions referred to in Article (41) above within 90 days of the date of the transaction resulting from any of the following cases:

- A third party might have accessed their account illegally;
- A third party might have known their account personal identification number (PIN);
- The client knows that an operation was performed through their account either without their consent or knowledge, or by mistake, or illegally.

The client is deemed to have notified the institution as per the previous subsection if they have followed the rules and procedures issued by the Banque du Liban.

Article 47:

In the event any of the institutions referred to in Article 41 above is informed of an unexecuted electronic payment operation or transfer, or of any of the cases described in Article 46 above, the concerned institution shall investigate the matter and advise the client in writing of the result. In all cases, the concerned institution has the burden of proving the contrary of the client's claims.

If the investigation shows that there is indeed an unexecuted operation or that one of the cases that should be reported under Article (46) occurred, the duly informed institution take the following actions and the client shall not incur any related fees or expenses:

1- Assume full responsibility by duly performing the unexecuted operation at the soonest.
2- Take the appropriate measures to protect the client's account.
3- Correct any error or reverse any illegal transaction.
4- Compensate for losses charged to the client's account, if any.

Article 48:

The orders to perform electronic payments and transfers shall be made in writing and shall be manually or electronically signed, under penalty of nullity.

If orders are electronically signed, the signature shall be authenticated in accordance with the rules issued by the Banque du Liban.

Article 49:

An electronic payment or transfer order may not be revoked after that the transaction amount was withdrawn from the sender's account, unless approved of by the beneficiary and the institution referred to in Article 41 above.

Periodic orders to perform electronic payments or transfers may be revoked provided that the institutions referred to in Article 41 above receive the revocation request at least two business days prior to the date of the next transfer.

Article 50:

The institutions referred to in Article 41 above shall be responsible for the non-execution or partial execution of electronic payment or transfer orders, unless they prove one of the following events:

1- The non-execution is due to an error, negligence, lack of orders or bad faith by the client.

2- The funds available in the client's account are not enough to execute the transaction, unless otherwise agreed with the client.
3- Occurrence of force majeure or an event beyond the control of the institution, provided it has made every reasonable effort to avoid such event.
4- Other events defined by the Banque du Liban.

In case the aforementioned institutions were proven to be liable for the non-execution or partial execution of the transaction, they should return the disputed amounts to the client and compensate him for the damage incurred where appropriate.

Article 51:

The institutions referred to in Article 41 herein may not collect fees, expenses, commissions or taxes related the electronic payment or transfer amount, unless they explicitly advise the client and obtain their written approval thereof.

Article 52:

The institutions referred to in Article (41) of this Law shall provide the client, in writing, with periodic statements of the transactions performed to his account, including information about the electronic payments or transfers debited and credited to their account, and the dates and value of such transactions.

Section II:

Bank Cards

Article 53:

The application submitted or agreement signed to be issued a bank card shall be in writing, and the issuing entity of the bank card should comply with the Banque du Liban regulations.

A BDL-licensed bank or institution may not issue or deliver an activated bank card to any person unless they apply for it or sign an agreement to receive it, except in the case of renewal or replacement of a pre-agreed card.

Article 54:

The entity issuing the bank card shall:

1- Provide the card owner with identification information that enables them to use it.
2- Ensure the confidentiality of the identification information provided to the card owner under subsection (1) above, by using a fit-for-purpose, up-to-date IT system.
3- Maintain complete statements on the transactions completed using the card for a duration specified by the Banque du Liban.
4- Provide the card owner with the appropriate means to report the card loss or theft.
5- Prevent any use of the card right after the loss or theft thereof has been reported.

The issuing entity shall deliver or send immediate notifications of transactions completed using the card, the main information about the payment or transfer transaction, such as the date and client's identity.

Article 55:

The card owner should use the card in accordance with the agreed conditions and take all the required precautions to protect the card and the relevant identification information.

The card owner may only revoke the electronic payment order or promise to pay made through the card upon approval of the beneficiary and the issuing entity.

Article 56:

In addition to cases where institutions are to be notified and the results thereof as stated in Articles (46) and (47) herein, the card owner shall notify the issuing entity verbally, in writing or electronically, of the of the card loss or theft immediately upon noticing the theft or the loss. The issuing entity shall deactivate and prevent the use of the card and any information allowing third parties to use it illegally, fraudulently or in any of the two cases stated in Article (58) below.

Article 57:

The card owner shall not be held accountable for the card loss, theft or illegal or fraudulent use by a third party provided that they immediately notify the institutions referred to in Article (41) herein, in writing or electronically, within the time limit specified by the Banque du Liban. In this case, the issuing entity shall have the amount of the fraudulent transactions refunded to the card owner's account no later than one month from the date of notifying the issuing entity, and the card owner shall not incur any additional financial liability.

The card owner shall be fully liable if the relevant institution proves that they committed a serious error or gross negligence or acted in bad faith or did not meet the obligation of duly notifying the institution as per the provisions of the above subsection.

Article 58:

The card owner shall not be held accountable for the following if they have notified the issuing entity thereof, in writing or electronically, and within the time limit specified by the Banque du Liban:

1- Illegal or fraudulent payment transactions executed remotely, without physically presenting the card or identifying the identity of the card holder.
2- Payment transactions executed using a forged card, in case the original card was still in the owner's possession at the time of performing the contested transaction.

In both cases, the issuing entity shall have the disputed amounts refunded to the owner’s account within a time limit of no more than one month from the day it was notified, with no financial liability incurred by the card owner.

Article 59:

The card issuing entity shall be liable for the bad or non-execution of the card owner's orders, the transactions executed without their approval, and/or errors in the management of their account.

Article 60:

Provisions set forth in section I of the present Chapter and relating to electronic payment transactions and electronic money transfers, shall apply to bank cards to the extent they do not contradict with the provisions of the present section.

Section III:

Electronic and Digital Money

Article 61:

The regulations issued by the Banque du Liban define the electronic and digital money, how to issue and use the same and the technical systems and regulations governing this type of money.

Section IV:

Electronic Checks, Check Digital Copies, Check Digital Representations and Digital Checks

Article 62:

An electronic check is a type of checks that is electronically generated, signed and negotiated.

A check digital copy is the scanned image of the paper check. Such copy is associated with full technical guarantees according to the Banque du Liban regulations.

The check digital representation is the process of extracting any or all of the information of the paper check in accordance with the Banque du Liban regulations.

The Banque du Liban has set out a definition of the digital check concept, how it is issued and used, and what are the technical systems and regulations governing the use thereof.

Both the electronic and paper checks shall include all the information referred to in Article 409 of the Code of Land Trade before converting the paper check into a digital copy.

Section V:

General Provisions

Article 63:

No right granted to any person, under the provisions of this Chapter, may be assigned, and any clause or agreement whereby a party assigns any such right, shall be considered void.

Article 64:

The general provisions relating to the bookkeeping of the bank transaction entries shall apply to electronic transaction entries and signatures.

The Banque du Liban may issue regulations related to the rules set forth in this Chapter, particularly in terms of governing payment orders, electronic and digital money, electronic transfers and checks, check digital copies, digital checks and digital representations, methods of issuing and using checks, rules of bookkeeping bank transaction entries and duration thereof, and the required protection and safety measures.

Part III:

Public Communication through Digital Means

Chapter I:

General Provisions

Article 65:

Public communication through digital means is any material that is digitally made available to the general public or groups thereof, including any type of signs, writings, images, recordings and messages that do not fall under the category of private correspondences.

Article 66:

Public communication through digital means is free to the extent permitted by the Constitution, the laws and the public order.

Article 67:

If any contract concluded under this Part is governed by a foreign law, it is mandatory that any business activities associated with such contract remain subject to the provisions of the Lebanese law to the extent they relate to:

1- Anti-competitive practices;
2- Rights protected by intellectual property laws;
3- Arbitrary clauses that constitute a prejudice to consumer protection;
4- Public order rules governing the practice of trade business.

Chapter II:

IT Service Providers

Article 68:

Network service providers and data hosts are both considered IT service providers.

Article 69:

Network service providers shall not be bound to monitor the information they send or store temporarily, but shall be bound to immediately remove or prevent access to such temporarily stored information upon the sender's request or a decision by the competent court, under penalty of law.

Article 70:

Data hosts shall not be bound to monitor the information they store in order to make it available to the public. However, they shall be bound to remove or prevent access to such information immediately once they become aware of its illegal nature.

Article 71:

The same person may be a network service provider and a data host at the same time.

All such activities qualify as e-commerce and shall be governed by Articles (30), (31) and (32) of the present Law.

Article 72:

An IT service provider shall save the traffic data of all the persons using their services, the data that help identify such persons and other technical data of communications, for three years as of the service delivery date.

After notifying the competent judicial authority, the judicial police may request the IT service providers, as part of its criminal investigations, to store additional technical data on a given incidence or specific individuals, other than the data prescribed in subsection (1) of this Article, for no more than thirty days considering the urgent nature of this data and the potential loss or modification thereof. Furthermore, such data may only be submitted to the Judicial Police upon a decision by the competent judicial authority.

The IT service provider may not invoke any technical failure causing the technical data not to be saved, and shall take the appropriate technical measures as defined in a decision by the Minister of Telecommunications.

The IT service provider shall be bound by professional secrecy to preserve the confidentiality of the technical data. However, the IT service provider may not invoke such secrecy before the competent judicial authority to the extent that the investigations and trials require the disclosure of such confidential data.

The data storage obligation set forth in subsection (1) does not include any stored or transferred content that expresses the views of its author, such as exchanged correspondences or content of stored/transferred information or websites.

The mechanism for saving/deleting traffic data and the nature of such data shall be defined by a decree issued by the Council of Ministers upon a proposal by the Minister of Justice.

Article 73:

The IT service provider shall be accountable to their clients for the good fulfilment of its contractual obligations.

The contracts with clients and appendices thereof shall define the service level, type and duration.

The IT service provider is partly or completely relieved of liability if the contract bad or non-performance is proved to be caused by an error committed by the client, a force majeure or an action by a third party.

Article 74:

Any professional who makes information available online to the public shall also include the personal identification details as stated in Article (31) herein.

A non-professional who makes information available online to the public may maintain anonymity and only make the data host identification details available to the public. They shall also provide the data host with their personal identification data as prescribed in Article (31) above, and the data host shall store the same for ten years.

Article 75:

The IT service provider, regardless of their nationality or principal place of business (in case of a legal entity), is deemed to have elected domicile in Lebanon to practice their business if they are permanently residing there.

Article 76:

IT service providers shall collaborate with the competent court and authorities stated in Law no. 99/140 to the extent needed to uncover the truth in investigations and pending lawsuits.

The competent court and authorities identified in Law no. 99/140 and to the extent permitted by said law, require the IT service provider to submit any data they store or control in case it is deemed helpful in any investigation or pending lawsuit, in accordance with the obligations stipulated in Articles (72) and (74) above.

The IT service provider, upon a decision by the competent court or judicial authorities stated in Law no. 99/140 and to the extent permitted by said law, shall immediately provide such authority with traffic data and other technical data as set forth in Articles (72) and (74) herein and grant them real-time access to any communication performed through the provider's network.

Article 77:

The breach by the IT service provider of any of the obligations stipulated in Articles (72), (74) and (76) herein constitutes a misdemeanor and is punishable by imprisonment of three to six months and/or a fine of ten million to fifty million Lebanese pounds.

Part IV: Website Names

Article 78:

The codes (.lb) and (.لبنان) refer to the internet country code top-level domain (ccTLD) for Lebanon.

Article 79:

Under the present Law, a body shall be established under the name of the "Lebanese Domain Name Registry" (LBDR).

LBDR's mandate is to manage and register the names of websites, including websites featuring the Lebanese domains (.lb) and (.لبنان) in their names, by conducting the required investigation and in consideration for a fee that fairly reflects the development of the registration market.

LBDR shall be comprised of representatives from the Ministry of Telecommunications, the Ministry of Economy and Trade, the Ministry of Finance, the Ministry of Justice, the Minister of State for Administrative Development, the Telecommunications Regulatory Authority, the Federation of Chambers of Commerce, Industry and Agriculture, the Bar Association and representatives of three to five associations operating in this sector. These representatives will be nominated by LBDR which also reserves to right to replace associations that become non-operational.

Article 80:

LBDR shall define the administrative and technical terms and conditions for granting and managing the Lebanese domain names and accredit registrars subject to the rules set out by the international domain name registration bodies.

LBDR shall include all such terms and conditions for domain names in one document and make them publicly available on its website.

Said document shall include objective, non-discriminatory terms and conditions for domain names, in conformity with the public order, the applicable laws and the rules and regulations set out by the relevant international bodies.

The Minister of State for Administrative Development shall manage and register the government domain names in coordination with the relevant ministries and departments.

Article 81:

Domain names may be registered and managed remotely through electronic means.

A domain name shall be registered without prejudice to third party rights.

In case of violation of the present provisions, the domain name applicant shall be legally liable where necessary, and such violation may cause the cancellation or transfer of the domain name.

Article 82:

Disputes over the domain names shall be referred to courts.

LBDR shall not be considered party to the dispute, but it shall enforce any decisions taken by the Lebanese courts to this effect.

Reconcilable disputes over domain names may be settled by non-judicial methods. The entity authorized to grant and manage domain names shall elect one or more arbitration centers to settle the disputes over the domain names by non-judicial methods.

The decisions reached by the arbitration bodies shall be effective and immediately enforceable through the competent enforcement bodies.

The domain naming terms and conditions available online should include a list of potential arbitration centers and their rules to settle disputes.

Article 83:

The entity authorized to grant and manage domain names does not acquire any rights arising from the exercise of its functions of granting or managing domain names.

Said entity shall not be responsible for the words and expressions chosen by applicants, provided that they comply with the domain names terms and conditions.

Article 84:

The entity authorized to grant and manage domain names may cancel or reject domain names, at its own discretion, in case the owner does not pay the due fees; or if the applicant for registration does not meet the requirements to benefit from a domain name; or if the information provided is incomplete, incorrect or outdated; or if the chosen words or expressions for the name violate the public order or the public morals.

The domain names terms and conditions shall define the rules of automatic cancellation or rejection of a domain name and the duration given to the non-compliant applicant to submit their remarks.

The fees are set by virtue of a decree issued by the Council of Ministers upon the proposal of the Minister of Finance.

Part V: Personal Data Protection

Section I: General Provisions

Article 85:

The Provisions contained in this Section shall apply to all automatic and non-automatic processing of data of a personal nature. However, the said Provisions shall not apply to the processing related to the personal activities carried out by the individual exclusively for fulfillment of his/her needs.

No agreement shall be made to contravene the Provisions of this Section which govern the rights of the persons concerned with the processing and the obligations of those responsible for such processing, and no agreement, any contravening clause or any undertaking pursuant to sole discretion shall be invoked.

Article 86:

Everyone shall have the right to review and object, before the personal data processing officer, to the information and analyses used in the automated processing related thereto, which are invoked thereby.

No judicial or administrative decision requiring an assessment of human behavior may rely solely on an automated processing of data that is aimed at identifying the qualities of the person or assessing certain aspects of his/her personality.

Section II: Collection and Processing of Personal Information

Article 87:

Personal data shall be collected faithfully and for legitimate, specific and explicit purposes.

The data shall be appropriate, not go beyond the stated objectives, be correct and complete and remain on a daily basis as relevant as possible.

At a later stage, the said data may not be processed for purposes that are not in line with the objectives specified, unless this is related to processing data for statistical or historical purposes or for scientific research.

Article 88:

The personal data processing officer, or the representative thereof, shall inform the persons from whom the personal data are derived of the following:

1. Identity of the data-processing officer or the identity of the representative thereof;
2. Objectives of the processing;
3. Mandatory or optional nature of answering the questions raised;
4. Consequences of non-response;
5. Persons to whom the data is to be sent; and

6. Right to access and correct information and the means prepared for the same.

The forms used for data collection shall include an explicit and clear statement of the information specified in Paragraph I of this Article.

Article 89:

When personal data is not collected from the person concerned, the data-processing officer shall inform the latter personally and explicitly of the content of the data, of the objectives of processing and of his/her right to object to conducting the processing.

This mandatory requirement shall be waived when the person concerned is aware of the matter or when informing him/her is impossible or requires an "effort" that is not commensurate with the benefit of the conducting.

Article 90:

Retention of personal data shall not be legitimate except during the period specified in the declaration of processing or in the decision authorizing the same.

Article 91

No data shall be collected or processed in the event it reveals, directly or indirectly, the health status, genetic identity or sexual life of the person concerned.

This prohibition shall not apply in the following cases:

1. In the event the person concerned has made such data available to the public or has explicitly agreed to process the same, unless there is a legal impediment;
2. In the event data collection or processing is necessary to establish a medical diagnosis or to provide medical treatment by a healthcare professional;
3. In the event a right is proved or defended before the court; and
4. In the event of obtaining a license in accordance with the Provisions of Article 97 of this Law.

Article 92:

Every natural person shall have the right to object, for legitimate reasons, before the data-processing officer to the collection and processing of his/her personal data, including the collection and processing for the purpose of commercial promotion. However, a person shall not be entitled to exercise the right of objection in the following two cases:

1. In the event the data-processing officer is obliged to collect the data under the law; and
2. In the event s/he has agreed upon processing of his/her personal data.

Article 93:

The personal data processing officer shall take all measures, in light of the nature of the data and the risks resulting from processing thereof, in order to ensure the integrity and security of the data and to protect the same against being distorted, damaged or accessed by unauthorized persons.

Section III: Actions Required to Implement Processing

Article 94:

No permit or license shall be required to process personal data in the following cases:

1. In the case of processing by the common rights officials, each as per his/her jurisdiction;
2. In the case of book-keeping, by Non-Profit Organizations (NPOs), of the members and clients thereof within the scope of their normal and legal exercise of their functions;
3. In the case of processes the subject thereof is keeping of dedicated records, under legal or regulatory provisions, in order to inform the public, which can be accessed by any person or persons having a legitimate interest;
4. In the case of processes the subject thereof is pupils and students by educational institutions for educational or administrative purposes of the said institutions;
5. In the case of processes the subject thereof is the parties or members of the institutions, commercial companies, trade unions, associations and self-employed persons, within limits and for the needs of exercising their activities in a legal manner;
6. In the processes the subject thereof is the clients and customers of institutions, commercial companies, trade unions, associations and self-employed persons, within limits and for the needs of exercising their activities in a legal manner;
7. In case the person concerned agrees in advance to the processing of his/her personal data, unless there is a legal impediment; and

In addition, some processes, or certain categories thereof, may be exempted from the authorization or licensing procedures in the event it is deemed that implementing the same shall have no risk to private life or personal freedoms, under a decree approved by the Council of Ministers at the proposal of the Minister of Justice and the Minister of Economy and Trade.

8. In the case of processes provided for in Law No. (99/140), and within the limits thereof.

Article 95:

With the exception of the exemptions provided for in the Preceding Article, those wishing to collect and process personal data shall inform the Ministry of Economy and Trade under a permit issued duly against a receipt.

Article 96:

The permit submitted to the Ministry of Economy and Trade in accordance with the Preceding Article shall include the following information:

1. Objectives of the process;
2. Personal data, and the source thereof, under processing;
3. Categories of persons concerned;
4. Third parties, or the categories thereof, who can view the data;
5. Data retention period;
6. Identity and address of the data processing officer;
7. Identity and address of the representative of the data processing officer in the event the said officer is residing outside the Lebanese territory;
8. Agency or agencies assigned with implementing the processing;
9. Person or agency exercising the right of access and how they exercise the said right;
10. Subcontractor, if any;
11. Where appropriate, method of access, or any other form of connection between data and other processes, as well as possible data waivers to third parties;
12. Where appropriate, transfer of personal data to another State in any form;
13. Actions taken to ensure the integrity of data of a personal nature and to ensure preservation of secrets protected under law, which are to be properly implemented by the data processing officer; and
14. Emphasizing that the processing shall be carried out in accordance with the law.

Article 97:

Personal data processes pertaining to the following shall be subject to licensing:

1. External and internal security of the State under a joint decision of the Minister of National Defense and the Minister of Interior and the Municipalities;
2. Penal offences and judicial proceedings of various kinds under a decision issued by the Minister of Justice; and
3. Cases of health, genetic identity, or sexual life of persons under a decision issued by the Minister of Public Health.

The license decision shall be issued within two (2) months from the date of submission of the application, otherwise it shall be deemed implicitly denied upon expiry of the deadline.

The Ministry of Economy and Trade and the applicant shall be notified in writing of the license or denial thereof.

Article 98:

The Ministry of Economic and Trade shall make available to the public, especially on its website, a list of possible processes that meet the licensing or authorization requirements set forth in this Section.

This list shall define, for each authorized or licensed processing, the following:

1. License or permit granted, the date thereof and the date of commencement of the processing;
2. Name and purpose of the processing;
3. Identity and address of the data processing officer;
4. Identity and address of the representative of the data processing officer in the event the said officer is residing outside the Lebanese territory;
5. Personal data categories under processing;
6. Person or administration exercising the right to access the data;
7. Third parties, or the categories thereof, who are authorized to view the data;
8. Where appropriate, personal data intended for transfer to a foreign State.

Section IV: Right of Access and Correction

Article 99:

Each personal data owner, or any of his/her heirs, shall have the right to inquire from the data processing officer about processing of the personal data in order to determine whether his/her data is under a processing or not.

The personal data processing officer shall provide the owner of the personal data, or any of his/her heirs, with a copy of the data belonging thereto at his/her request. In case such data is encoded, compressed or encrypted, the owner of the data of a personal nature, or of any of his/her heirs shall be given an understandable copy.

The owner of the data of a personal nature, or any of his/her heirs, may also request the data processing officer, in accordance with the conditions specified in Paragraph II above, to hand over the following additional information: the purposes, categories, source, subject and nature of the processing, identification of the persons and their categories to whom the personal data is being sent or those who can access the same, as well as the timing and purposes of such access.

Article 100:

The personal data processing officer may receive a payment for giving a copy of the personal data belonging to the owner thereof, or any of his/her heirs, as provided for in the Preceding Article, provided that the payment shall not exceed the cost of copying.

The personal data processing officer may object to requests of an arbitrary nature, in particular with regard to the number or repetitive or systematic nature thereof. When a dispute arises, the burden of proving the aforementioned arbitrary nature shall lie upon the personal data processing officer receiving the same.

Article 101:

The owner of a personal nature, or any of his/her heirs, shall have the right to ask the data processing officer processing, correcting, completing, updating and erasing of such data, which is incorrect, incomplete, ambiguous, expired or incompatible with the purposes of processing, or the data that are not to be processed, collected, used, saved or transferred.

In the event the personal data subject of the request of correction has been sent to a third party, the data processing officer shall notify the latter of the amendments made at the request of the owner thereof or any of his/her heirs.

The personal data processing officer shall, at the request of the owner of the data or any of his/her heirs, perform the required operations free of charge within ten (10) days from the date of submitting the correction request and shall prove his/her performance of the required.

The personal data processing officer shall automatically correct the said data when s/he is informed of one of the reasons requiring him/her to modify or cancel the said data.

Article 102:

To the owner of the personal data, or to any of his/her heirs, may resort to the competent courts, in particular the Magistrate of Summary Justice in accordance with the dispute rules in order to ensure the exercise of the right of access and correction and to report the application of the Provisions of this Section in respect of personal data relating thereto.

Article 103:

In the event the processes are related to internal or external security of the State, the owner of the data of a personal nature shall not be informed of his/her data under processing in case this may endanger the objectives of the processes or the internal or external security of the State.

Article 104:

The right of individuals to access the public records and files and the medical files containing personal data shall be subject to the legal and regulatory provisions that govern the same.

Article 105:

The Provisions of Articles 99, 100 and 101 of this Law shall not apply to the processing of data of a personal nature carried out solely for the purposes of literary and artistic expression or for the purposes of the professional exercise of a journalistic activity within the limits of the laws in force.

The Preceding Paragraph shall not preclude the application of laws that observe the conditions of exercise of the right of response, which regulate exposure to private life and the reputation of persons.

Section V: Penal Provisions

Article 106

The following shall be penalized with a fine from one (1) million Lebanese Pounds to thirty (30) million Lebanese Pounds and imprisonment from three (3) months to three (3) years or with one of the following two penalties:

- Anyone who has processed personal data without providing a permit or without obtaining a prior license before commencing its work in accordance with the Provisions of Section III of this Chapter; and
- Anyone who has collected or processed personal data without complying with the rules established in accordance with the Provisions of Section II of this Chapter;
- Anyone who, even if negligently, discloses personal data under processing to unauthorized persons;

Article 107:

Any personal data processing officer who refuses to respond within ten (1) working days or who responds incorrectly or imperfectly to the request of the person concerned, or his/her agent, regarding the aforementioned right of review or correction shall be liable to a fine of one (1) million Lebanese Pounds to fifteen (15) million Lebanese Pounds In Section IV of this Chapter.

Article 108:

In the event of recurrence of any of the acts provided for in this Section, the penalties and fines provided for in the aforementioned Articles shall be increased by one third to one-half.

Article 109:

The criminal proceedings under Paragraph III of Article 106 and Article 107 shall be carried out only on the basis of a complaint by the damaged compliant.

The general right shall be waived in accordance with the waiver of the personal right in respect of such criminal acts in case such waiver occurs before the judgment in the case becomes final.

Part VI: Crimes Relating to IT System and Data; and Bank Cards; and Amendments to the Penal Code and Rules of Procedure for IT Evidence Control and Storage

Chapter I:

Crimes Related to IT Systems and Data

Article 110: Illegal Access to an Information System:

Any person who fraudulently accesses, enters or stays in an IT system, or parts thereof, shall be liable to imprisonment for three months to two years and/or a fine of one million to twenty million Lebanese pounds.

Such penalty shall be increased to imprisonment for six months to three years and a fine of two million to forty million Lebanese pounds if this act results in cancelling, reproducing or amending digital data or software, or in jeopardizing the operation of the IT system.

Article 111: Compromising System Integrity:

Any person who fraudulently damages or hinders the operation of an IT system in any manner, shall be punished by imprisonment for six months to three years and/or by a fine of three million to two hundred million Lebanese pounds.

Article 112: Compromising Digital Data Integrity:

Any person who fraudulently enters digital data into an IT system or deletes/modifies digital data hosted by such system, shall be punished by imprisonment for six months to three years and/or by a fine of three million to two hundred million Lebanese pounds.

Article 113: Hindrance, Disturbance or Disruption:

Any person who hinders, disturbs or disrupts, intentionally and by any means, the access to the service or hardware, software, data sources or information through the use of the information network or a computer or any other similar means, shall be punished by imprisonment for three months to two years and/or by a fine of two million to thirty million Lebanese pounds.

Article 114: Misuse of Hardware and IT Platforms:

Any person who imports, produces, acquires, delivers, disposes of or publishes, without a legitimate reason, any hardware, software, IT platform or any developed or adapted data, with the intention to commit any of the offenses listed in the preceding articles of this Chapter, shall be punished by imprisonment for six months to three years and/or liable to a fine of three million to two hundred million Lebanese pounds.

Article 115:

Any person who attempts to commit any of the offenses stated in this Chapter shall be liable to the same penalties.

Chapter II:

Counterfeiting and Forgery of Bank Cards and Electronic and Digital Money/Checks

Article 116:

Any person who:

1- Counterfeits or forges a bank card;
2- Knowingly uses or trades with a counterfeit or forged bank card;
3- Accepts to receive amounts of money knowing that payment was made using a counterfeit or forged bank card;
4- Counterfeits electronic or digital money;
5- Knowingly uses counterfeit electronic or digital money;
6- Counterfeits an electronic or digital check;
7- Knowingly uses an counterfeit electronic or digital check;

shall be punished by imprisonment for six months to three years and/or by a fine of ten million to two hundred million Lebanese pounds.

Provisions of Articles (114) and (115) shall apply to the offences stated in this Article.

Chapter III:

Non-Observance of the Rules Applied to Electronic Commerce

Article 117:

Any person who violates the obligations imposed upon an originator of a SPAM message, as set forth in Article (32) herein, shall be punished by a fine of two million to twenty million Lebanese pounds.

Chapter IV:

Publishing by Electronic Means (Electronic Publishing)

Article 118:

Subsection (3) of Article (209) of the Penal Code shall be amended as follows:

"Writing, drawings, paintings, pictures, films and various types of signs and photos, in case they are displayed in a public place, a place open to or seeable by the public, or in case they are sold, offered for sale or distributed to one or more persons by whatever means, including electronic means".

Chapter V:

Electronic Forgery

Article 119:

Article (453) of the Penal Code shall be amended as follows:

"Forgery is deliberate distortion of the truth by changing the facts or data established by an instrument, manuscript, paper/electronic medium or any other medium that forms a document, with a view to cause physical, moral or social damage".

Chapter VI:

Exploitation of Minors in Pornographic Materials

Article 120:

Subsection (3) of Chapter II of Part VII titled: "Offences against Public Morality" of the Law issued by Legislative Decree no. 340 dated 01/03/1943 (Penal Code), shall be repealed and replaced by the following provisions:

"Subsection (3) – Crimes of Minors' Exploitation for purposes of Pornography

Article 535 – Minors' exploitation for purposes of pornography means photographing, showing or physically depicting any minor through whatever means, such as drawings, photos, writings, films or signs showcasing the minor's sex organs or the minor himself/herself while engaging or acting as though engaging in explicit sexual activities.

The Penal Code provisions shall apply to offences relating to minors' exploitation for purposes of pornography (if validated), without prejudice to the provisions of the following Article.

Article 536 – The development or production of pornographic materials effectively involving minors is considered as a form of human trafficking, and the perpetrator of such crime shall be punished in accordance with Articles 586 (1) onwards on human trafficking of the Penal Code.

If minors are not effectively involved in such pornographic material, the perpetrator shall be punished by imprisonment for one to three years and by a fine of five hundred thousand to two million Lebanese pounds.

Any person who delivers, communicates, reproduces, displays, disposes of, distributes, exports, imports, posts, transmits or promotes minors' pornography by whatever means, shall be punished by imprisonment for one to three years and by a fine of five hundred thousand to two million Lebanese pounds.

Penalties set forth in this article are increased in accordance with Article 257 (Penalties) in case of the use of an electronic communication network such as the internet, radio or TV broadcasting to publish or distribute minors' pornography to an unspecified audience.

The same penalties shall apply to attempts to commit the crimes set forth in the preceding subsections.

Notwithstanding anything to the contrary herein, any person who regularly takes or displays pornographic materials involving minors, via radio/TV broadcast, a communication service targeting the general public, or any other means, or deliberately holds any such materials, shall be punished by imprisonment for no more than one year and/or a fine not exceeding two million Lebanese pounds.

The provisions of this article shall be applied to pornographic images of any person looking like a minor.

In case the criminal offence set forth in this article are committed by a legal entity, it shall be suspended from work for one month at least and two years at most".

Chapter VII:

Rule of Procedure for Seizing and Retaining IT Evidence

Article 121:

IT traces are the data created voluntarily or not by persons on the systems, databases, IT services and networks. IT traces are considered digital or IT evidence.

IT evidence includes: hardware, software, data, applications, IT traces and the like.

SoPs prescribed in this Chapter shall be followed to seize IT evidence upon a decision by the Public Prosecution or the competent judicial authority.

The privacy of the IT evidence shall be protected, particularly the data and images that are not related to the criminal case.

The Judicial Police shall take the standard procedures to seize and retain IT evidence as prescribed in this Chapter, upon a decision by the competent judicial authority.

A specialized office shall assist the Judicial Police in seizing and retaining IT evidence.

Article 122:

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.

Article 123:

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 offences, particularly Articles (33) and (41) thereof.

Article 124:

Seizure of data and software shall be conducted in a manner not compromising the rights of good faith persons and the person directly involved, by copying the seized data and software only. In other terms, the hardware containing the seized data and software shall not be seized, especially when such hardware is used for other legitimate purposes.

At the time of seizure, in case of downloading or transferring data/IT evidence from a website or a computer, the source thereof shall be specified.

Any data or digital evidence stored in an IT system located in the Lebanese territories may be seized 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, if they are made available to the public or in case the legally authorized person approves of disclosing such data through an IT system in the Lebanese territories.

When the IT evidence is seized, the Public Prosecution or the judicial authority examining the case may decide that the process of downloading, transferring or copying data/software shall be done in the presence of the relevant person or any specialized technician appointed by the relevant person under a written authorization.

Where appropriate, the scene where the search operations are conducted or the location of the electronic medium containing the data/software shall be closed and sealed pending the arrival of the technician within the specified time limit. Otherwise, the search operations may take place in the presence of two relatives of the concerned person, their lawyer or two witnesses. Nevertheless, the competent judicial authority may decide that their presence is not necessary.

A copy of the seized data/software may be given to the concerned person at the time of seizure, by decision of the judicial authority taking such action.

The judicial authority may request any person who knows how to operate the IT system or protection measures thereof, to provide the investigator in charge with the required information to access the requested data and software.

It may also request any person having data or software that could serve as IT evidence, to make and hold a copy thereof until seizure is decided.

Article 125:

The court examining the case may order, in its final decision, the suspension of certain electronic services, block certain websites or cancel accounts on such websites in case they are associated with crimes relating to terrorism, Minors' pornography, prohibited gambling, organized electronic frauds, money laundering, crimes against internal and external security or crimes of compromising IT system integrity such as spreading viruses.

Article 126:

The Public Prosecution may decide to temporarily suspend certain electronic services, block websites or freeze accounts in such websites for no more than thirty days. Such period may be renewable only once through a justified decision and this action will legally cease to have effect upon expiry of the time limit.

The investigating judge or the competent court examining the case may decide on such actions temporarily pending the final decision on the case. The judicial authority may also reverse its decision in case of new compelling circumstances arise. The decision of the investigating judge and the court to suspend certain electronic services, or block websites or freeze accounts on such websites, may be duly challenged within the time limits of the release decision.

Article 127:

Any evidence seized or retained in breach of the the provisions in this Chapter are considered invalid, and, the corresponding investigation shall be revoked.

However, evidence invalidity shall not prevent the use of any information deemed helpful for the investigation in case such information is uncovered as a result of seizing or processing the invalid evidence, provided that it is accompanied by corroborative evidence.

Part VII:

Amendments to Consumer Protection Law no. 659 dated 04/02/2005

Article 128:

The following subsection shall be added to Article (51) of the Consumer Protection Law no. 659 dated 04/02/2005:

Electronic contracts shall be concluded pursuant to the provisions of Articles (33), (34), (35) and (38) of the Electronic Transactions and Personal Data Law.

Article 129:

Article (55) of the Consumer Protection Law no. 659 dated 04/02/2005 shall be repealed and replaced by the following provision:

Notwithstanding anything to the contrary herein, any consumer who enters into a contract in accordance with this Chapter may reverse their decision to buy/hire goods or benefit from a service within a period of ten days starting from the date of concluding the contract for services or delivery date for goods, unless the parties agree to longer periods under the contract.

However, the consumer may not exercise the right set forth in the preceding subsection in the following events:

1- If they benefit from the service or use the goods before the elapsing of the ten-day period.
2- If the contract includes goods made to order or according to specifications defined by the consumer.
3- If the contract involves video tapes, discs or CDs: In case their covers have been removed.
4- If the contract involves the purchase of newspapers, magazines and other publications.
5- In case the goods become defective due to bad maintenance by the consumer.
6- If the contract involves accommodation, transport, food or entertainment services delivered on a specific date or periodically at agreed-upon intervals.
7- If the contract involves the purchase of software services online, except when the software is not downloaded or functional.

Article 130:

Article (59) of the Consumer Protection Law no. 659 dated 04/02/2005 shall be repealed and replaced by the following:

Any professional who uses indirect or electronic means for sale or lease shall abide by the provisions of this Law, particularly in relation to deceptive advertising, promotion and public safety.

Part VIII:

Final Provisions

Article 131:

The COLIBAC BoD shall also include a Director representing the Ministry of Telecommunications and appointed in accordance with Article (5) of Law no. 572/2004.

Article 132:

The enforcement of the present Law shall comply with the provisions of the Banking Secrecy Law promulgated on 03/09/1956, the provisions of Article (151) of the Code of Money and Credit, the provisions of Act no. 133 dated 26/10/1999 on the General mission of Banque du Liban, the provisions of Law no. 140, dated 27/10/1999, related to the protection of secrecy of communications (carried out by all communication means) and the code of ethics relating to any relevant profession.

Article 133:

By way of exception from the provisions of Article (20) and onwards in Chapter IV of the present Law, the Banque du Liban may grant the following in relation to financial and banking transactions:

1- Certificates of authentication for electronic signatures to banks and institutions supervised by Banque du Liban and the Capital Markets Authority, and to institutions, departments and bodies dealing with Banque du Liban under the laws governing its [i.e. BDL] operations.
2- Accredited certificates to banks and institutions supervised by Banque du Liban and the Capital Markets Authority in its capacity as provider of authentication services for electronic signatures for its customers.

Banque du Liban sets the technical standards and rules of the procedures set forth in this Article.

Article 134:

Subject to the provisions of Article (64), details of enforcement of the present Law shall be defined, where necessary, by decrees issued by the Council of Ministers upon the proposal of the Minister of Justice, the Minister of Economy and Trade, the Minister of Finance, the Minister of Industry and the Minister of Telecommunications, each within the limits of their competences.

Article 135:

Electronic commerce activities shall be subject to taxes and fees imposed on non-electronic activities in accordance with applicable laws, subject to Law no. 44 dated 11/11/2008 (Tax Procedures Law) and its amendments, particularly pertaining to the Tax Administration's right to obtain information.

Article 136:

The present Law shall be effective three months after publication thereof in the Official Gazette.

Rationale for the Electronic Transactions and Personal Data Draft Law

In the past years, the world has witnessed a revolution in the field of Information Technology and its uses in electronic transactions. In fact, electronic transactions have grown after the emergence and steady expansion of the internet, and they are now used as a universal market to promote goods and deliver services, thus representing the key component for developing the electronic commerce.

E-transactions have become a daily fact in Lebanon, but they are carried out under no legislative framework as the applicable Lebanese laws did not keep up with the developments by finding adequate legal solutions. It is therefore critical to recognize and accept the electronic documents and signatures as a means of proof considering the ever-accelerating trend towards paperless contracts and documents. It is now also essential to regulate the processing of personal data processing and enforce adequate legal controls to preserve individuals' privacy and personal freedoms. Furthermore, the sector involving electronic commerce and transactions, communication service delivery, data hosting and granting (.lb) and (.لبنان) domain names need to be regulated through legislations and controls that protect transactors and citizens, provided that such controls do not hinder the development of the e-commerce and e-transaction sector, so as not to discourage investments that would otherwise benefit the national economy at large, especially that both the internet and the e-transactions are open and of a cross-border nature.

The present draft law consists of eight parts covering the themes addressed above. The content of each part is outlined below:

Part I tackles the legal provisions on electronic writings and evidence. Legal rules under this Part recognize the electronic documents/ signatures and grant an electronic written document the same power of proof granted to a paper document, in case it satisfies certain conditions. They also make it possible to approve of official electronic documents pursuant to a decree issued by the Council of Ministers. This step will allow the management to make the required preparations and develop the required controls and safeguards. This Part also deals with various issues such as: storing electronic data, disputes over written evidence, the multiple copy rule of ordinary documents, denial or alleged forgery of electronic documents and signatures, protection measures for electronic writings, role of electronic authentication service providers and their accreditation by COLIBAC and conditions thereof…

Part II deals with the electronic commerce. It outlines the obligations binding all e-commerce practitioners; sets out the regulations governing electronic offerings; defines the specific provisions on electronic approvals, the contracting party's electronic instead of handwritten statements, and SPAM messages. As for electronic banking services, this Part

addresses electronic payment orders, electronic transfers, bank cards, electronic money, electronic checks, as well as banks, financial institutions and clients obligations/responsibilities and agreements signed in this respect. It concludes by highlighting the powers of Banque du Liban in this regard.

Part III of the Law sets forth the legal provisions on Public communication through digital means, i.e. the obligations and responsibilities of technical service providers (network service provider or data host). It also governs the process of making information anonymously available to the public online.

Part IV regulates how (.lb) and (.لبنان) domain names on the internet are granted and managed. It also sets out the national administrative, technical and legal requirements as well as the requirements and approvals prescribed by the international domain names registration entities. This Part also discusses the role of the Lebanese institution authorized to grant and manage domain names, outlining its rights and responsibility for the words and expressions used in domain names, and in cases of revoking the granted domain name. Part IV also deals with the settlement of disputes over domain names by non-judicial methods or in the competent courts.

Part V provides comprehensive legal regulation for personal data protection. It defines the objectives and limitations of processing personal information, cases where processing of such information is legally banned, the method by which personal information is collected, and the obligations and responsibilities of persons processing the data. This Part also includes a lengthy list of processing practices that do not require authorization or licensing.

Part V also defines the rules governing the authorized/ licensed processing of data and how to apply for authorization before the competent authority. It also addresses the legal rights of the person whose data is being processed: their rights to object to and inquire about the processing; request information thereon; and request correction, update, completion or deletion, etc. of their information.

Part VI deals with the crimes related to IT systems and data, bank cards and certain amendments to the Penal Code (Legislative Decree no. 340 dated 01/03/1943). This Part also includes penal provisions on crimes related to IT systems and data, counterfeiting or forgery of bank cards and non-compliance with e-commerce rules and regulations. It also includes amendments to the Penal Code in connection with Article (209) on publication means and Article (453) on forgery.

Part VII includes amendments to certain provisions of the Consumer Protection Law no. 659 dated 04/02/2005 to ensure consistency with the e-commerce provisions.

Finally, Part VIII provides some concluding and transitional provisions related to the present Law, particularly in terms of compliance with the Banking Secrecy Law and other laws, and defining Banque du Liban powers of licensing and authentication of electronic signatures used in the financial and banking sector.

Therefore,

Considering the foregoing, the Government has prepared the enclosed draft law and presently submits the same to the honorable Chamber of Deputies for adoption.