International Telecommunication Union

Cloud Computing in Arab States: Legal and Legislative Aspects, Facts and Horizons

International Telecommunication Union Report

By: Dr. Janane EL-KHOURY

Beirut, December 30, 2015

PLAN

Executive Summary

This study aims at reviewing the legal and legislative aspects of cloud computing in the Arab States facts and horizons, and the multi-faced issues it raises - legislative, executive, administrative, technical and practical, in addition to other issues such as cloud computing security, data protection, processing and transfer, apps security and identity management system. The legal aspect of cloud computing is basically tridimensional: the functional and technical dimension, the legal dimension and the contractual dimension. Therefore, it is important to discuss whether there is an official (local and regional) Arab vision to set up a digital infrastructure for integration into the international digital environment, especially considering several concerns over such service in the Arab States mainly related to data security; Internet violation or weak Internet-based services; environmental concerns; contracts of adhesion imposed by the service providers which impede the movement of data, procurement of services and functioning applications. These concerns cause the Arab region to lag behind in this domain. Other legal, objective and procedural issues have also been raised, from the extent of cooperation among Sates, mainly on technical issues; the extent of cooperation among the local competent ministries; the cooperation between the public and private sectors; the financial cost for the Arab States for the integration to cloud computing; capacity building in Arab States and an academic university major, the raising of public awareness and the dissemination of a national and regional culture of cloud computing. However, what matters the most is the issue of sovereignty over databases. In fact, there are contractual challenges and several concerns particularly about where to keep the data and by what legislation should it be covered.

To discuss all these issues, it is important to review and update the legislative framework of cloud computing in the Arab region in general, and at the national level for the 22 Arab States (Jordan, United Arab Emirates (UAE), Bahrain, Algeria, Kingdom of Saudi Arabia (KSA), Kuwait, Tunisia, Comoros, Djibouti, Syria, Sudan, Somalia, Iraq, Sultanate of Oman, State of Palestine, Qatar, Lebanon, Libya, Egypt, Morocco, Mauritania and Yemen), by studying the following points, mainly: the concept of cloud computing; the legal, technical, administrative, political and practical risks; and best practices in cloud computing (the European Union and US experiences). Suggestions and recommendations such as an Arab Safe Harbor are presented, as well as the active role of the ITU, with the conclusion including some findings and proposals with a focus on the future.

Introduction

Every human generation has its own stake, around which all organizations, negotiations and structure of the aligning of balanced international relations, directly or indirectly, revolve. Today, the globalization of technology has primary influence on the development of the global society, and its major production is what is known today as cloud computing. Cloud computing is considered as one of the greatest technological transformations and breakthroughs in the world, offering many long-term and large-scale services on the web, particularly services related to data storage, backup, networks, cybersecurity, management systems, data transmission, use and development of software, creation of job opportunities, and the development of the ICT industry.

On the other hand, cloud computing creates lots of challenges in the Arab States in general, and in every single country in particular, mostly at the legislative, executive, administrative, technical and practical levels, in addition to the loss of data control[1], and the efforts necessary to ensure that the operations of cloud computing are in line with the existing local and regional legal regulations and rules[2]. Also to be considered are other issues such as cloud computing security, data protection, processing and transmission, application security, material security and identity management system. The legal aspect of cloud computing is located in three dimensions: functional and technical, legal and contractual. This is why many international organizations that are watching over security and evolution of the international community - including the ITU - are working to find new technical, legal, administrative and practical frameworks for cloud computing, in order to assure privacy of the personal data that may belong to individuals, companies and countries, by reconsidering the current situation at the national level and the applicable rules related to the cloud computing.

Internationally speaking, the world is currently oriented towards cloud computing services. Several countries, particularly the developed ones, such as the United States, the European Union countries and China, elaborated national strategies and policies aimed at taking benefit from cloud computing services, particularly at regulating their relations with large corporations which requires an extended infrastructure, local data centers, in addition to small and medium sized enterprises. In the Arab States, the international reports[3] show an annual constant cloud computing usage growth. Therefore, it is important to discuss its status in these States, and whether there is an official Arab (national and regional) vision to lay a digital infrastructure for the integration into the continuously and fast changing digital world. Considering the several concerns about such service in the Arab States, related to the information security, the information safety for governmental data, the breakage of the Internet service or the non-adequacy of the services in addition to the environmental concerns, the adherence contracts imposed by the service providers on the local clients, or the sudden ban imposed by the companies on the Software as (SaaS) services, or the Platform as (PaaS) service, or the Infrastructure as

(IaaS) service, which hampers the movement of data, procurement of services and functioning of applications and thus keeps the Arab region backward in this area. There are also several legal, objective and procedural difficulties[4], the question of the extent of cooperation amongst these States, mainly technical problems[5], the extent of cooperation amongst the national competent ministries, the cooperation between the public and private sectors, the financial costs of engagement of the Arab States in the cloud computing world, the issue of specialized capacity building in the Arab States and a specialized academic college, the public awareness, and the spread of a national and regional culture of cloud computing.

Still the most important issue is related to the national sovereignty over the databases[6]. There are contractual challenges and concerns especially concerning by what legislation should data be covered - is it the law of the host country in the name of national sovereignty or that of the company's head office - and what is the possibility of executing a judicial order rendered by the local courts against such companies.

To discuss all the above issues, the legislative framework of the cloud computing in the Arab region in general, and in the 22 Arab States (Jordan, United Arab Emirates (UAE), Bahrain, Algeria, Kingdom of Saudi Arabia (KSA), Kuwait, Tunisia, Comoros, Djibouti, Syria, Sudan, Somalia, Iraq, Sultanate of Oman, State of Palestine, Qatar, Lebanon, Libya, Egypt, Morocco, Mauritania and Yemen), must be reviewed. This requires studying the following points: concept (definition) of cloud computing, and its scope, characteristics, features, components, types and models; taking into consideration risks, concerns and fears related to the weak infrastructure, the information security, the situation of the specialized companies, the applications and costs in some States, the necessary measures and controls, the extent of cooperation amongst the specialized international organizations, the specialized large corporations. In addition to the legal, technical, administrative, political and practical problems and their risks[7], the best practices in cloud computing (European Union and American Western experiences), the effective role of ITU in the Arab States, and providing with several suggestions concerning the contractual dimension of the cloud computing and recommendation to establish an Arab safe harbor before ending up with some conclusions and suggestions with a focus to the future.

Part I: Cloud Computing and its practical and legislative aspects

Historically, the word "computing" dates back to the 1960's when John McCarthy said: "Computing may someday be organized as a public utility." Such computing was compared to the utilities such as gas and electrical power. There was a debate about the Cloud Computing, and about whether it is a series of techniques, or of services[8], or of activities, or of applications, or of different technologies or market offers, which made its definition complicated, especially that every time the different viewpoints regarding its definition became closer, its services get developed, changed and expanded, which makes it once again impossible to agree on one common and unique definition. Thus, there are multiple definitions because of the multiple definers. It is therefore difficult to come up with a clearly worded definition, that can be used by everyone as a basis and starting point to identify the legislative framework of the cloud computing. For example, cloud computing, as defined by ITU, is "a model that enables the service users to have ubiquitous, convenient and on-demand access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or introduced by the service provider[9]. Cloud computing enables the performance of the cloud computing services."

In fact, there are three major types of cloud computing services: Infrastructure as a service - IaaS, Platform as a Service - PaaS and Software as a Service - SaaS.

There are also three cloud computing types: Private Clouds, Public Clouds and Hybrid Clouds.

The cloud computing providers are those who provide cloud computing services to individuals and companies and even to the States wishing to purchase or rent such services, while being under the responsibility of ensuring the continuity and maintenance of the services 24/24 and 7/7. The main providers are: Google, Salesforce, GoGrid, Vmware, Rackspace, Amazon.

The most important cloud applications and services are: e-mailing services (Yahoo - Gmail - Hotmail), cloud storage services (Dropbox - SkyDrive - Google Drive - Box), cloud music services (iTunes/iCloud - Amazon Cloud Player - Google Music - Music Creator), cloud applications (Googles Docs - Photoshop Express - Pixlr Editor - Jaycut - Aviary) and cloud operating systems (Google Chrome OS - Jolicloud).

As far as the scope of the cloud computing is concerned, several surveys showed a constant growth over the last years and in the years to come[10]. As for its characteristics, like any production of the digital globalization, it features many advantages in terms of management, cost-efficiency, company and data, mainly: easy access to the data, databases and applications, time and cost saving (cost of hardware), no costs incurred for equipment & furniture, archive storage space, release from the pressure and the obligations of commercial laws (trademark, trade register, …), release from office work,

ensuring incessancy of services, insurance and protection, as well as other economic and commercial benefits provided by the cloud computing systems. The cloud computing is the gold mine of the 21st century and a technology that will change the game rules. Nelly Kroes, vice-president of the European Commission, confirmed that cloud computing services offer huge advantages to citizens and trading companies, and reinforce the European economy in general[11]. While the European studies warn against "the security risks of the cloud computing", for the information belonging to corporations, persons and even individuals were directly or indirectly accessed by specific parties, thus violating the privacy and resulting in many security consequences, although the European Union is protected by lots of instructions, recommendations, laws and bilateral agreements, the question is still open: What about the Arab States? For many of these States do not intend to start using the cloud computing for the reasons that will be listed below.

Clause I: Practical Challenges and Legal Issues of Cloud Computing in Arab States:

Many States are reluctant to decide to adopt the cloud computing for the following reasons:

- The disability to get the latest developed applications and software at reasonable prices; the neglect of some States and regions where Internet service is not available; the need for a digital storage space that can contain the large amounts of stored archives and most importantly the security and confidentiality of the private information of individuals, companies and governments.

- The absence of the tax administration with respect to any sale, assignment or purchase of a database[12], thus causing the Treasury to lose tax revenues particularly in the States where taxes are a major resource.

- The persistent reluctance of the Arab local policymakers, national, administrative and political decision-makers to move to cloud computing and take advantage of its services.

- The suspicious protection and insurance capacities of the providers of cloud computing services.

- The distrust in the service providers[13], the new technologies and the competency of cloud computing service providers.

- The lack of awareness amongst officials and decision-makers about the importance of the virtual moving to cloud.

- The insufficient progress made to establish a large-scale local broadband network; non applying of restrictive policies on the web content; the discrimination towards the foreign technology corporations and the lack of an appropriate framework for the information and communications technology standards.

- The slow or/and costly Internet connection in some countries; the lack of a digital infrastructure in the Arab countries (the Internet service outage means the suspension of the cloud computing services. In fact, the interruption of Internet may cause some companies to lose millions, if not billions of dollars in few minutes).

- The insufficiency of information security in cloud computing (all the companies' personal information and rented services are available outside the organization). The very confidential and top secret information of some private companies cannot be risked and placed in rented data centers no matter how reassuring the providers of such services all over the world are, in addition to risks related to information security in digital clouds, and which can be caused by both the service provider and the client. Therefore, the service provider has the main obligation of laying a sophisticated infrastructure, and safe tools and data-centers, especially if the storage is not for free (while the client has only to ensure a quick Internet connection).

- The lack of information security in relation to some of the governmental institutions (which is a major reason for the reluctance of many Arab countries in the use of cloud computing).

- The environmental concerns, considering the large amounts of power consumption for the big data-centers.

- The lack of publicity and awareness-raising about the importance of the use of this technology[14], which means there is a lack of awareness among Arab public opinion about how to use such data and recognize the possible risks surrounding the data security, and the true value of such data which are considered as "new oil" from a commercial point of view, and whether consumers should have economic rights in return for the trade of their data[15].

Here below are detailed the reasons stated above:

Practical Challenges of Cloud Computing in Arab States:	
• Disability to get the latest developed applications; • Absence of the tax administration; • Hesitation of the political decision-makers; • Suspicious protection and insurance capacities; • Distrust in the service providers; • Absence of the big data-centers	• Lack of awareness; • Insufficient progress; • Slow or/and costly Internet connection; • Lack of a digital infrastructure; • Insufficiency information of cloud computing; • Lack of the needed publicity.

Clause II: Legislative and Regulatory Situation Exclusively in Arab Countries

The legislative issue of the cloud computing brings up lots of problems particularly in the Arab countries[15] where no particular laws were enacted to protect the databases and the data in general. Principally, few Arab countries have adopted special law dedicated to personal data protection. There are only fragmented texts introduced in separate legislations. Moreover, most of the Arab countries have no mechanisms to apply the elaborated rules concerning the protection and execution of such data. In addition, the local and sovereign traditional principles now face a challenge and a constant clash between the respect of the public freedoms and the requirements of the security and public safety. The issue of the determination of the limits within which liberties and privacies must be respected and how to prevent excessive verification and interference by the public authorities and others became problematic.

At the common law level, many of laws in the Arab countries have been amended, particularly the criminal law and the law on civil procedure, in order to include the legal protection of information, data, intellectual property and digital documents. Moreover, many laws have been enacted with respect to the information technology, the electronic transactions, the e-commerce and the cybercrimes in the Arab countries in order to incriminate many computer-based acts committed in the cyber space, as well as other web and ICT-related crimes, and to deal with the digital and physical acts on an equal footing. The Gulf Cooperation States are among the first Arab countries that have paved the way for the cloud computing. (The Arab States will be listed alphabetically).

Summary of the Legislative and Regulatory Situation of Cloud Computing in Arab States

Name of the State	Cyber-Legislation and Regulations	Code of Conduct	National Strategy to move to Cloud computing	Training and Awareness
Algeria	-Law n°4/2009 - Other draft-laws	Non-existent	National strategy (2014-2020) including cloud computing and e-administration	Insufficient training and awareness
Bahrain	Communication and Intent Law n°48/2002, law n°28/2002 on e-transactions and e-commerce, law n°60/2014 on IT crimes, decree n°9/2002 on reorganization of the Central Informatics Organization and 2005 law n°25 on formation of a supreme committee for IT and communications.	Non-existent	A project launched in 2015 to enhance cloud-computing based transactions.	Insufficient training and awareness
Comoros	Non-existent	Non-existent	Non-existent	Non-existent
Djibouti	Law of 2008 on consumer protection	Non-existent	National initiatives	Insufficient training and awareness
Egypt	Constitutional Principles; Telecommunications Law of 2003 and law n°120/2008 on establishment of economic courts, specialized draft laws. Decree on IT crimes of 2005; Draft laws	Non-existent	Administrative initiatives and signing of expertise-exchange international memorandums of understanding.	Organization of trainings and awareness-raising sessions.

Iraq	Law n°1/2010 on consumer protection, law n°78/2012 on e-signature and e-transactions.	Non-existent	National Strategy and action plan of Iraqi e-government (2012-2015)	Insufficient training and awareness
Jordan	Temporary law on public statistics 2008, Law n°30/2010 on software crimes; Law n°21/2011 on communications and telecommunications.	Non-existent	Cloud computing platform launched in 2014; statement of the General Government Policy in communications and information technology; establishment of the IT Center.	Specialized training and general awareness-raising needed.
Kingdom of Saudi Arabia (KSA)	Kingdom's anti-cybercrime regulation of 2007; Cabinet Decision n°40/2006 on control of state e-transactions; decision n°6667 on conditions of practicing as consultant in communications and information technology; draft Law on data protection	Non-existent	Administrative and political will to start using cloud computing; formation of the Communications and IT Authority.	Insufficient training and awareness
Kuwait	1999 law n°5 on protection of literature and computer against software and data base; law n°37/2014 on creation of the Communications and IT Organization Authority; draft law on e-transactions	Non-existent	National initiatives	Insufficient training and awareness
Lebanon	Law n°140 of October 27, 1999 on protection of the right to confidential phone conversations; draft law on e-transactions and cybercrimes	Non-existent	A national strategy drawn up in 2012 for the protection and safety of cyberspace in Lebanon. Launching of the digital communications vision for the year 2020.	Insufficient training and awareness
Libya	Draft laws on cyber-crimes and e-transactions	Non-existent	"E-Libya initiative"	Insufficient training and awareness
Mauritania	Draft law on the "legal framework of the Mauritanian Information community.	Non-existent	Governmental initiatives	Non-existent
Morocco	Constitutional principles on protection of confidentiality; law n°7/2003 on anti-cybercrimes; law n°53.05 on e-exchange of data; and law n°31/ 2008 on consumer protection on internet.	Non-existent	Governmental initiatives	Insufficient training and awareness
Palestine	General statistics law n°4/2000 on the right to access statistical information; e-transactions law of 2010; decree n°35/2004 on the right to access the world web. Cabinet decisions in Palestine on the right to access the world wide web (internet) and e-mail via the state computer center; on banning of sale and marketing of communications and IT and express mail services.	Non-existent	- National strategy for telecommunications and information technology. - The E-Palestine Initiative	Insufficient training and awareness
Qatar	Qatar Constitutional Principles of 2003 on individuals' privacy; Telecommunications law n°34/2006; e-transactions and e-commerce law n°16/2010 (August 19, 2010); QFC' law n°7/2005; data Privacy draft-law	Non-existent	State Cloud computing strategy: National Strategy for Cyber Security (2014)	Insufficient training and awareness Research about cloud computing
Somalia	Non-existent	Non-existent	Non-existent	Insufficient training and awareness

Sudan	Sudanese Constitutional Principles on Confidentiality and privacy, E-transactions law of 2007 and anti-cybercrime law of 2007.	Non-existent	Governmental initiatives	Specialized trainings and awareness raising sessions
Sultanate of Oman	E-transactions law (69/2008), anti-IT crime law n°12/2011	Non-existent	Governmental Will	Insufficient training and awareness
Syria	Law n°4/2009 on digital signature and web services; law n°18/2010 on organization of the communications industry; Information law under decree law n°108 of August 8, 2011; decree law n°17/2012 on organization of the web communication and fight against cybercrimes.	Non-existent	IT National Strategy (2004) E-government National Strategy (2009-2010)	Insufficient training and awareness
Tunisia	Law n°63/2004 on personal data protection; law n°38/1998 on the mail magazine; law n°83/2000 on electronic exchange and commerce; law n°2331/2000 on control of the financial and administrative organization and facilitation methods of the National Digital Certification Agency; order n°1967/2001 on control of digital certification services; order n°1968/2001; law n°5/2004 on regulation of the information security; law n°51/2005 on e-transfer; directive n°13/2007 on establishment of the digital economy; order n°1274/2007 on the list of digital economy-related activities.	Non-existent	National strategy for Cloud Computing (2015)	Starting specialized training and awareness-raising campaigns.
United Arab Emirates (UAE)	Emirates Telecommunications Corporation act n°1/1991; act n°3/2003 on regulation of the telecommunications sector; law of 2002 on e-commerce and e-signature; federal law n°1/2006 on e-transactions and e-commerce; Dubai law n°2/2002 on e-transactions and e-commerce; federal law n°2/2006 on anti-cybercrime; federal decree law n°5/2012 on fight against cybercrime; circular n°6/2013 on Abu Dhabi Government policies and standards on information security; Emirate Cabinet Decision n°21/2013 on the information security list in federal governments; personal data protection DIFC law n°1/2007; personal date protection law n°11/2006; Dubai act on data publication and exchange (open data law of October 17, 2015); 2002 Dubai act on telecommunications network creation and protection; law n°5/2004 on cybersecurity; Executive council decision n°13/2012 on Dubai information security.	Exist but require updating	National strategy and administrative rules for cloud computing	Starting specialized training and awareness sessions
Yemen	Law n°40/2006 on methods of payment for electronic banking and financial transactions; Cabinet decision n°4/2002 on establishment of the City of Communications and Information; draft law on information protection.	Non-existent	Cloud computing-based technical services	Insufficient training and awareness.

I. Jordan

On the administrative level, in June 2014, the Ministry of Communications and Information Technology of Jordan launched the "special cloud computing platform" which was developed in collaboration with Microsoft in support of the needs of public sector and of the emerging companies that suffered from lack of supportive infrastructure to develop their ideas and products such as software and electronic services. Moreover, an agreement was signed between Umniah, the mobile operator r in Jordan and Microsoft to provide cloud computing services to the company. In October 2015, the Specialized Technical Services Company (STS) launched its own platform of cloud computing solutions which allows its services and products to be provided through the cloud. This is in addition to initiatives taken since 2014 to apply the education cloud solutions technologies in some Jordanian schools and which enable users to access them from school or home via smartphones or tablets.

On the legislative level, the Jordanian legislator enacted in 2008 the temporary law on public statistics which includes articles on the secrecy and protection of the statistical data, and prevention of their disclosure (art. 11, 12, 16, 17 and 51). In 2010, Information System Crimes Law n°(30) of 2010 was promulgated (official gazette n°5056 dated September 16, 2010 - page 5334), this law embodies two types of substantive and procedural rules including the crimes committed by using information systems including violation of privacy, disclosure of data or information by illegally accessing a computer system, disclosure of data or information by introducing, publishing or using software, wiretapping of electronic correspondences.

Jordan has enacted the telecommunications law n°13/1995, which was rectified by amendment law n°21/2011 (official gazette n°4072 of October 1st, 1995). This law includes terms on competition in information and communication technologies sectors, as set forth in articles 6, 12, 26 and 28, as well as terms on the licensing of communication networks, renewal, modification and cancellation of licenses, control of licensors and protection of beneficiaries.

In 2003, the Jordanian government adopted the Statement of Government Policy on the Information and Communications Technology Sectors & Postal Sector which focused on the liberation of the entire telecommunications sector. In 2007, the government approved a new policy focused on the competition in the telecommunications sector and the adoption of an integral licensing system, in addition to provide some radio frequencies to be used through the open public licensing. At the end of 2012, the Government approved the currently applicable Statement of Government Policy which highlighted the effective competition and integration issues[16].

Jordan also set up the National Information Technology Center which serves as the ICT executive authority in State institutions in matters concerning the exploitation of ICT resources and the determination of its standards. Jordan has also established a "National Center for Security and Crisis Management" (Official Gazette n°5335, n°20 of 2015), aimed at providing relief in disasters and crisis management.

II. United Arab Emirates (UAE)

The UAE has been witnessing major regulatory and administrative shifts towards cloud computing, and it is currently one of the largest GCC markets as its market has been valued in 2015 at 5 billion AED. According to experts, all projects of public and private sectors in UAE have been undergoing dramatic technological changes in terms of the use of the cloud computing solutions, the accelerated dissemination of cloud-based applications that would meet the business needs, the faster response to the new trading opportunities thanks to the cloud solutions, the merging of the cloud's general services and the on-site applications for a solid infrastructure of the information technology, the exploitation of the infrastructure as a service and the software as a service to promote competency and productivity and an innovated business model, and the creation of new revenues for the secondary markets.

On the legislative level, no legislation on data protection has been enacted in UAE, though the right to privacy is established in the UAE constitution and other laws. Under this constitution, the individual shall be "free to communicate by mail, or by telegraph, or by any other communication means and the confidentiality of such communications are guaranteed by the law". In addition, the UAE penal code (n°3/1987) stipulates specific rights to privacy and personal data protection (articles 327 to 330, chapter V, on family crimes - and article 279 of the UAE penal code on crime of violation any of the communication and telecommunication means).

The UAE has issued the "Emirates Telecommunications Corporation" act (n°1/1991), the first law that regulates the communication and telecommunication affairs within the State. This act created Emirates Telecommunications Corporation, set its goals, objectives and functions, and gave it the exclusive right to transmit communications and telecommunications, and to operate, maintain and develop the general communication system within the State, and also between the State and parties abroad. The chapter XVI thereof comprises the sanctions inflicted in case of non-abidance by its provisions (articles 45 and 46).

This act was followed by act n°3/2003 on regulation of the telecommunications sector, amending some provisions of the "Emirates Telecommunications Corporation" act and organizing the telecommunications companies' work within the State. Under the act, a new authority was established: the Telecommunication Regulatory Authority, and in article 12 thereof, the tasks, powers and functions of the authority are identified, and the authority is defined as the authority that controls the telecommunications sector. Chapter 9 thereof includes articles incriminating some acts and inflicting sanctions in case of non-compliance with the provisions and obligations as provided for by the act (articles 71 and 72).

In 2002, Dubai act n°2 on e-transactions and e-commerce[17] was enacted in order to develop and promote the e-commerce by making electronic correspondences easier, to transfer e-documents, to clear any impediments to the application of the e-commerce and e-transactions, to minimize any possibility of e-fraud, to renew the public confidence in the information safety and authenticity (article 3), to set the e-transactions requirements (article 7), to make electronic contracts and ensure their authenticity (articles 13 to 18), to organize the creation of protected digital records and signatures (articles 19 to 22), to determine the provisions related to certificates and certification services (articles 23 to

26), to promote the State use of digital records and signatures and accept depositing and issuance (article 27). The said law also identified the sanctions resulting from committing any act that constitutes a crime under the applicable legislations by use of any electronic means (article 28 to 35).

The UAE also enacted federal law n°1/2006 on e-transactions and e-commerce[18] to protect the rights of online dealers and determine their obligations (article 3), to accept the e-transaction (article 6), the electronic literature and signature (articles 8 and 9) and the electronic evidence and its authenticity (article 10). The law also provided for the conclusion of electronic agreements and their authenticity (article 11), the trusted e-transactions (article 12), the outsourcing (article 13), the acknowledgment of receipt (article 14), the time and place of message delivery and receipt (article 15), the protected electronic registers and signatures (articles 16 and 17), the reliability of the electronic signatures and certifications (article 18), the site's electronic obligations (article 19). Moreover, the law includes the provisions related to the e-certifications and the legalization services and their control (articles 20 and 21), the recognition of foreign electronic certifications and signatures (article 23), the State use of electronic records and signatures (articles 24 and 25) and finally the sanctions enforced in case of violation of the applicable legislations on the use of electronic means (articles 26 to 33).

There is also the Federal Law n°2/2006 on Combating Cybercrimes[19], which is considered as a model law in the Arab countries. The law encompasses most of the cybercrimes, including illegal access to a website or software by logging in the site or the software, transgression of an authorized access, infringement of personal data, cancellation, omission, destruction, disclosure, modification or republishing of data or information.

The Union also passed Federal Decree-Law n°5/2012[20] on Combating Cybercrimes, as a replacement for Law n°2 of 2006, but with no stipulation as to what specific procedures the criminal investigations[21] should follow.

This is a modern law to fight cybercrimes, as it incriminates the access to any website or electronic information system or information network or information means without a permit or the abuse of such permit (articles 2 and 14), the prevention of such access (article 8), or the disabling or blocking of same (article 10), or the access to government data or financial or economic confidential information (article 4), or to medical or health-related information (article 7), the alteration or destruction of a website (article 5), the falsification of State e-documents (article 6), the fraud against the IP address (article 9), the committal of crimes such as electronic fraud (article 11), or electronic blackmail (article 16), online gambling or crimes against the code of ethics (articles 17 to 20), acquisition of digital money (articles 12 and 13), interception of third parties communications (article 15), attack against private data (articles 21 and 22), human trafficking (article 23), creation of division or racism (article 24), arms trafficking (article 25), drug trafficking (article 36), smuggling of antiquities and artistic pieces (article 34), e-terrorism (article 26), other crimes against the State prestige and status and its local and international security (articles 28 to 32 and articles 38 to 44), or violation of sacred values and religious beliefs (article 35) and money laundering (article 37).

In 2013, the UAE issued circular n°6 on the Abu Dhabi government's data security policy and standards. Moreover, departmental order n°21/2013 on Information Technology (IT) security regulations at federal government entities was issued by the UAE Cabinet to enhance the information security concept, provide a legal framework to ensure the safety of the IT rules and set the standards of their optimal use, encourage the effective application of digital security and create a safe environment in the federal government entities to preserve the information and make sure the information and the network's main infrastructure are kept confidential.

It is worth noting that the UAE has set up Electronic Certification Center which developed the digital ID project and, in 2010, a decree was promulgated by the Emirates Telecommunications Regulatory Authority to control and minimize the undesired marketing communications.

In 2008, the UAE established the Computer Emergency Response Team, "aeCERT"[22], to enhance the standards and practices of the information security and to protect the ICT infrastructure against cyber risks and attacks.

The Dubai International Financial Center DIFC has also elaborated special law[23] on the protection of its own data and lists that are in harmony with the EC directive on data protection (EC/46/95)[24] and the directives of ESCWA and of OECD (Organization for Economic Cooperation and Development). However, such laws only apply to the activities of this financial center and the banking services or the transfers made from such centers outwards and for statistical purposes only.

And the Dubai Law on data publication and exchange (open data law of October 17, 2015)[25] has many of its terms dealing with the collection, legality and safe processing of data, and the updating of such data within a specific period (art.8), the explicit approval of the data owner and the necessity of processing (art. 9), the explicit written approval (art. 10), the appropriate protection during the transfer of data outside the country (art. 11 and 12), the right to access and correction (art. 17) and the responsibilities and obligations of the data protection commissioner (art. 18). The said law puts in place well-defined mechanisms and creates a specific committee for the Emirate of Dubai to control the data classification, set the standards of the databases there, follow their publication and exchange between the parties, facilitate their procurement, put in place unified storage and classification mechanisms and introduce consolidated data within one platform for all department in Dubai Emirate. The law also works on promoting competitiveness between the data providers, enhancing the transparency of the data exchange and ensuring harmony between the services provided and the privacy of the local authorities, thus creating an integral legislative environment, developing a new generation of integral smart solutions and completing the legislative building of the smart Dubai city.

Simultaneously, it is important to mention Dubai law issued in 2002[26] with relation to the establishment and protection of telecommunications network. On January 27, 2012, the

executive council issued departmental order n°13 on the data security in Dubai Emirate[27]. And in 2014, Dubai set up the "e-security and anti-cybercrimes center"[28].

III. Bahrain

In November 2015, in collaboration with Amazon Web, Bahrain launched, the first project to accelerate the business in the GCC countries from the Council's head office in Bahrain based on the cloud computing. This project aims at keeping up with the economic technologies and priorities since the cloud computing is a worthy replacement of oil for a sustained economy in the region, which motivates the Bahraini institutions to adopt digital technology and enhance national capabilities and the education as well.

Legislatively, Bahrain came up with a series of laws related to the cyberspace, mainly: the telecommunications and Internet law n°48/2002 which incriminates any alteration, interception or disclosure of communications and of their content (article 75 thereof). Under this law, the Communications Regulatory Authority (TRA) was set up to protect the personal data and the privacy of services, as well as the Bahrain Internet Exchange (BIX) (http://www.bix.bh) was established to control the licenses of the Internet service providers. However, the Bahraini code includes no terms on the information movement or the deletion by the service providers of the subscribers' processed and stored data once done with the e-mail services.

Bahrain also passed law n°28/2002 on e-transactions and e-commerce, law n°60/2014 on IT crimes and decree n°9/2002 on reorganization of the Central Informatics Organization (CIO) as well as decree n°25/2005 on the establishment of the High Committee on ICT.

IV. Algeria

Since 2014, the Ministry of Post, Information Technology and Communication of Algeria has been working on a strategy that is due to remain in effect up to 2020, covering the country in whole and including the cloud computing and the e-administration, with a view to advance the technology industry, modernize the Algerian economy, and prepare appropriate legislation and regulations to keep the data confidential and safe and to ensure the high level of confidentiality during digital correspondence exchanges.

Legislatively, an important reference must be made to law n°09-04 of 14 Shaaban 1430 H (August 5, 2009) which regulates prevention and fighting of IT-and communication-related crimes.

In fact, Algeria is preparing the "electronic authentication and signature" draft law which guarantees personal data protection and ease online information exchange, as well as another draft law concerning the e-transactions.

V. Kingdom of Saudi Arabia (KSA)

Practically, the cloud computing has been widely adopted in business and international investments in KSA and the ICT industry has witnessed a competition between the top companies specialized in information and communication technologies by offering the cloud computing private services. The cloud computing also extended to the public sector which is oriented to a new concept, i.e. Government Cloud (G-cloud), targeted at making the government bodies, such as ministries and public institutions, adopt the cloud computing and the virtual clouds, where all data are saved. Like any new concept, the cloud computing in KSA aroused concern and was sometimes faced with rejection by several private and public bodies due to information security-related warnings and fears with regard to leakage of crucial data from the cloud.

The Consultative Assembly of Saudi Arabia has formed the Communication and Information Technology Commission to discuss the regulations related to the provision of the cloud computing services in the Kingdom, to show the developed countries' experiences in the field of cloud computing and underline the main regulations and mechanisms to provide with such services whether in terms of operation or of the policies designed to offer the service or of the legal forms of such service. The committee warned against the risk for the Saudi individuals, governmental bodies and corporations to seek the cloud computing services from foreign companies, as this arouses concerns over the national security, the rise of demand for the international communication capacities, the dependency, the data protection and the possible outflows of funds and investments from the country.

Legislatively, the Saudi Arabia has no legislation on data protection, though the right to privacy is established in a number of laws, such as the major management law which mainly stipulates that all correspondences and communications between the parties must be completely confidential and not be disclosed. The courts of the Kingdom identify the violations of the secrecy of data according to the Islamic laws and have a wide discretionary power to estimate the means of such violations. Moreover, the tendency in the Kingdom is to acquire the approval of the data owner before proceeding to the disclosure of his/her personal data. There is currently a draft law under discussion at the Consultative Assembly of Saudi Arabia on data protection. The Kingdom also set up SA-CERT[29].

In the same context, the Kingdom's Anti-Cybercrime Law issued in 2007 (Royal Decree n°M/17 dated 8/3/1428 H) would sentence any person acting illegally to access the computer of another person with a view to omit, destroy, change or redistribute the information to a fine of SR /3,000,000/ maximum and/or to prison for no more than 4 years. Any person that accesses the bank or credit information of another person or any information about the securities owned by that person would be also sentenced to a fine of SR /2,000,000/ maximum and/or to prison for no more than 3 years.

In the same context, the Council of Ministers issued departmental order n°40 of March 27, 2006 on the regulations governing the public e-transactions, and departmental order n°6667 of 1/7/1426 H, on the conditions of practice of consulting in the ICT sector.

VI. Sudan

According to Sudan, the application of the cloud computing and the adoption of its techniques are among its strategies to plan for the sustainable development, as the awareness of the State officials has been raised as to the importance of the geo-information. In fact, the use of the cloud computing helps carry out the State's global strategy by unifying the e-government tools and software and the model applications. A geo-database is being established to make available to its users and the decision-makers a complete package of accurate information documented with photos in support of the sustainable development projects. There is also the Mobile Mapping service which consists of three operations: data collection, storage of data in a special center, and training of the body using the system.

Legislatively, in its article 29, the Sudanese Constitution stipulates the privacy and confidentiality of communication and correspondence, as well as the privacy of every human being. In 2007, Sudan enacted the e-transactions law and the counter-cybercrime law. Article 6 thereof evokes the crime of wiretapping, capturing or intercepting messages, without authorization from the Public Prosecutor, or the appropriate authority or the owner of the information and which is sanctioned with a sentence of prison of 3 years maximum or a penalty or both. Article 7 thereof refers to the deliberate access to websites for the purpose of getting security information or data about the country's national security or national economy and which is sanctioned with a sentence of prison of 7 years maximum or a penalty or both. However, if the access is for the purpose of canceling, deleting, destroying or altering data or information about the country's national security or national economy, it shall be sanctioned with a sentence of prison of 10 years maximum or a penalty or both.

On January 1st, 2010, Sudan created the Sudan CERT[30] Information Security Center which gives technical advice to citizens and corporations, assists the judicial staff and protects the main ICT structure in the country. Concrete achievements were made by the Center such as the detection and the countering of the serious computer virus Duku. The Sudanese e-government[31] has been launched.

In 2013, the implementation of the Training of Trainers program started for a safe use of the Internet, in addition to several awareness raising activities.

VII. Somalia:

Since the Somalian Constitution stipulates in article 22 the "correspondence freedom and its confidentiality", as well as all means of communication" and seen that the ICT sector is one of the best sectors in Somalia, there is a legal lack with regard to electronic transactions, the ICT regulation and the cybercrimes.

VIII. Iraq

The same applies for Iraq where only initiatives have been launched concerning the principle and the idea of using and exploiting the cloud computing and the databases, maintaining confidentiality and privacy and introducing its applications in the higher education in particular. Though the cloud computing can serve as a solution for several technical problems the information and communications technologies sector in Iraq suffers from.

However, at the legislative level, there is the trademarks and commercial data law n°21/1975, amended by law of January 4, 2010, not to mention the consumer protection law n°1 of January 4, 2010.

In 2012, Iraq passed law n°78 on the electronic signature and e-transactions[32], which recognized the digital bonds and regulates the terms thereof. The Republic of Iraq put in place the national strategy and the plan of action of the Iraqi e-government 2012-2015.

IX. Kuwait

Briefly, Kuwait has launched national initiatives to revitalize the electronic archive and cloud computing applications designed to keep up with the digital revolution, to provide practical solutions and effective strategies to administer the content, the digital ports and the storage and archive systems, as well as to discuss the technological and administrative challenges facing the public and private institutions in their transition to the digital environment. There is also the Kuwait Information Network[33] that interconnects around 56 public bodies in one automated network allowing them to transmit and exchange digital information and documents. The cloud computing techniques are likely to be used to activate the role of this Network, to achieve an important step in the development of ICTs in Kuwait, and to save the data and information on the cloud computing. Microsoft Office 365 was also launched to provide a number of computer and web-based applications and services.

Since its inception in 2006, the Central Agency for Information Technology (CAIT)[34] has been contributing in the implementation of several projects to build the necessary ICT infrastructure, and to develop the e-government system. There is also a draft Kuwaiti law on cybercrimes.

At the legislative level, Kuwait enacted the law by decree n°5/1999 concerning Intellectual Property Rights to ensure protection of information and computers including software and databases (art. 1).

Kuwait is also working on a draft law on the e-transactions where articles 35 to 40 state that the State departments or the public committees or institutions, or the companies, or the non-governmental authorities or staff of such authorities may not, illegitimately, access, or disclose, or publish any personal data or information registered in their digital records or information systems, save some cases and considerations related to the country's national security, in addition to other provisions.

In 2014, the Communication and Information Technology Regulatory Authority (CITRA)[35] was established in Kuwait by law n°37/2014. A Computer Incident Response

Team is being now developed to be part of the Central Agency for Information Technology (CAIT) with the aim to minimize the risks and security breaches, take precautionary measures, disseminate any information concerning any existing or potential threat, and coordinate the efforts to respond to emergency or e-risks, including practical, technical and procedural steps.

X. Morocco

The new Moroccan Constitution issued by Dahir (Moroccan king's decree) n°1.11.91 of 27 Shaaban 1432 H (July 29, 2011) stipulates in article 24 thereof that "the confidentiality of personal communications, of whatever form, shall not be violated, and any access to their content, the publication of such communications in whole or in part or their use against any person shall not be authorized unless by judicial order and according to the terms and methods provided for by the law." This principle was introduced in law n°03-03 on counter-terrorism before being adopted in the new Constitution, where article 108, section 1, of the Moroccan Code of Criminal Procedure, states that "it is forbidden to capture, register, reproduce or seize phone conversations or communications achieved through means of communication".

In 2009, the law n°08-09 on the protection of people from the processing of personal data[36] introduced for the first time in the Moroccan legal arena a series of legal obligations which are in tune with the international law, particularly the directive 95/46/EC on protection of personal data.

The law n°8 of the year 2009 is applied to the processing of personal data whether it concerns a specifically identified or identifiable person. For example, the name, the address, the e-mail, the photograph, the identity number and the fingerprints are all considered as personal data. The processing that concerns personal data protection includes every operation or the total operations that target personal data whether by automated means or other. This particularly concerns gathering, recording, organization, maintenance, adaptation or modification, extraction, browsing, use and disclosure by transmission or any other form of availability, approximation or linkage as well as blocking, scanning or destruction. In addition, it is worth noting that it takes only one of these operations for the processing of personal data to exist and to be subjected to the obligations of law n°09-08. In fact, the gathering of information without disclosing or publishing them is sufficient to single out the processing operation.

Moreover, this law does not only apply to companies and persons on the Moroccan territory, but also to all foreign companies having business with Moroccan peers or exchanging data with their Moroccan subsidiaries or parent companies via means that are available on the Moroccan land. However, this law excludes the data related to the exercise of personal or family activities, the data obtained from the administration of national defense and the State's interior and exterior security, as well as during the course of a processing that took place in application of a specific legislation.

The law incriminated in part 7 thereof a series of acts, including collection of personal data in a fraudulent or illegitimate manner, or processing of data for purposes other than those declared or authorized, or subsequent processing of the said data that is inconsistent

with the purposes declared or authorized, as well as transfer of personal data to another country in transgression of the provisions of articles 43 and 44 of the said law.

The law has also entrusted the National Control Commission for the Protection of Personal Data (CNDP) approved by the Prime Minister the task of activating the provisions of this law and the texts enforcing it and of watching over its compliance pursuant to article 27 thereof. Under article 45, this committee holds the national register for personal data protection.

Morocco also passed law n°07-03 as complementary to the laws constituting the criminal code related to crimes of breach of electronic data processing system. This law is restricted to the following criminal acts:

- Fraudulent access to the entire or part of the electronic data processing system;
- Persistence in the electronic data processing system after access by mistake;
- Omission or modification of the data included in the electronic data processing system or causing disruption in their functioning;
- Deliberate hindrance of the processing system functioning or causing dysfunction thereof;
- Unauthorized insertion, destruction, omission or modification of data;
- Falsification or counterfeiting of IT documents and use of same to harm third parties;
- Providing of equipment, tools or software designed for committing the abovementioned crimes.

In this context, there is law n°05.53 on the digital exchange of electronic data. It is a law that contains 43 articles on the following fields:

The regulation applied to the electronically exchanged data, the balance between hard copies and soft copies and the digital signature. It has also defined the legal framework applied to the operations made by the digital certification service providers and the rules that must be complied with by the said service providers and by the holders of the digital delivered certificates. In order to protect the e-transactions and the authenticity of the digital documents and digital signature, this law has incriminated in chapter 3 thereof concerning the punishments, the preventive measures and the detection of transgressions, a number of cybercrime forms, as they damage the trustworthiness of digital documents. Most of the punishments imposed with respect to the acts provided for in the law are for misdemeanors.

Then, the law n°31-08 which sets measures for consumer protection comes to support the Moroccan legal arsenal on the consumer protection including protection of the consumer online. The law guarantees to the consumers good information and adequate protection against unfair terms and some commercial practices. It also ensures complementary terms with regard to contractual guarantee, after-sale service and borrowing money.

In the same context, and given the important role of the consumer's movement in information, enlightenment and legal protection of consumer rights, the law has given the

public utility consumer associations the right to plead before courts in representation of the consumers' public interests.

XI. Yemen

In a practical research, Yemen launched a cloud computing-based TV service called Play Station. Legislatively, Yemen is preparing a 2009 draft law on information[37] in order to set the principles of the right to information access, its terms and procedures, the cost of information access, the exceptions to the right to information access within the limits allowed by the law, the parties to which the law gives this right, the information management, the tasks of the controlling and steering committee, the drafting and adoption of policies and plans in the information field and the pursuance of their implementation and the role of such committee in setting the basics and standards of data and information processing, in addition to the exchange of information between all the State apparatuses, the units of the public, mixed and private sectors, the foreign companies operating in the country. However, this draft law has failed to refer to the private data transfer and transmission outside the country; it should then be added before being finally approved.

Yemen passed law n°40/2006 on the regulations of payment, electronic financial and banking transactions, which stipulated the conditions of the transferability of the electronic bond and the payment methods, the electronic funds transfer and the electronic signature and register documentation measures.

In 1995, by presidential decree n°155/1995, Yemen established the National Information Center to keep up with the developments of the information society. In 2002, it established by virtue of the departmental order of the Council of Ministers n°4/2002, the Communication and Information Technology City in order to achieve the e-government and to form an integral technical community with communication and information technologies. It is worth noting that there are no explicit laws on the privacy in Yemen, and particularly the digital privacy.

XII. Tunisia

The first cloud computing site for institutions in Tunisia was launched in April 2015 in order to make it easy for the public or private institutions to reach the professional applications, so that the cloud computing can be available to different institutions and to provide a better network for saving, uploading, coverage and services.

Legislatively, since 1998, the IT and communication services, in general, and the postal services, in particular, have been identified and their good use and exploitation have been ensured under law n°38/1998 on the post magazine, in order to control the conditions of how to exercise the post activity, and guarantee the right of the public to the main postal services, while ensuring the confidentiality of the correspondences according to the legislation in force. In addition, the law n°19/1998 on rectification and completion of some provisions of the criminal law was passed as a way to protect data, digital services and software.

On the other hand, there is law n°83/2000 on electronic exchange and commerce, which handles with the general rules regulating the electronic exchange and commerce, and which are governed, insofar as they are contrary to the terms of the law, by the legislation and procedures in force. The law text states: "The e-contracts are subject to the written contracts regulation in terms of the expression of will, its legal effect, its authenticity and its enforceability in consistence with the terms hereunder". This law created "l'Agence Nationale de Certification Electronique".

Tunisia also enacted a series of laws, decrees and resolutions that constitute the legislative framework of the Internet uses and the related rights, mainly Telecommunication law n°1/2001 to regulate the communications field and provide the basic services of communications and TV and radio broadcasting. Under law n°1/2001, it set up the Communications National Authority which is empowered to give opinions about how to set the tariffs of networks and services, handle the local charts related to numbering and labeling, ensure the observance of the obligations resulting from the legislations and the hierarchy and look into the conflicts arising out of the setup, operation and exploitation of the networks.

Then in 2004, Tunisia adopted law n°63/2004 on personal data protection and which established the right of each individual to protect the personal data concerning his own life as they are basic rights guaranteed by the constitution and may only be processed in a transparent and honest manner and in such a way as to respect man's dignity.

In the same context, the Tunisian law n°5/2004 on regulation of the information security and control of the general rules to protect the computer systems and the networks, and which gave rise to the National Agency of Information Security (ANSI) entrusted with the general monitoring of software and networks with regard to the different public structures and vested with several powers including: executing a national strategy for the information safety by setting the necessary standards, preparing technical evidences, adopting information national solutions, conducting periodical examination for all public and private utilities and ensuring the technological vigilance. In 2007, the said agency created tunCERT[38]. In fact, several laws (laws n°1249/2004 and n°1250/2004) were subsequently enacted to put into force law n°5/2004.

Moreover, directive n°31 of 2007 was issued on the establishment of the digital economy which is considered as a national priority, the increase of the competitiveness of the national economy and its positive impacts on the different activities. The digital economy means the economy which involves ICT-based activities with high added values. A draft on the creation of the Tunisian Technical Agency for Telecommunications is under preparation to ensure that the Internet movement is legally controlled, in addition to another draft law on combating of IT and communication-related crimes.

XIII. Comoros

Based on an Internet research there is no publicly available information on legislation about cybersecurity or regulations or administrative rules about how to regulate the information and communications technologies in Comoros. L'Autorité Nationale de Régulation des TIC (ANRTIC) was established in May 2009 by virtue of decree n°65 to ensure the drafting of applicable policy and laws, to create a fair competition between suppliers and to protect the interests of the State and of the consumers[39].

In June 2015, the digital terrestrial television was launched in Comoros as an initiative to keep pace with the latest ICT development.

XIV. Djibouti

As a first initiative, in 2012 in collaboration with Ericsson, Djibouti has launched, the project of the use of the cloud computing solutions in education and telecommunication sectors for the provision of high quality educational services.

Legislatively, Djibouti passed law n°28/2008 on protection, suppression of fraud and consumer protection, where article 42 - clause 1 provides for the consumer consent protection with regard to the false and deceptive advertising which deceives consumers.

Djibouti also seeks to occupy a regional place in the communications industry and achieve the development vision. The ICT industry is a promising sector that would help advance the Djiboutian economy, and several effective partners in terms of Internet advancement. Djibouti is working in cooperation with the ITU to enhance the capacities of the information and communications technologies infrastructure[40], as well as with Bahrain and Egypt in the field of expertise exchange and the human capacity building.

XV. Sultanate of Oman

The Sultanate has enacted a series of legislations on the cyberspace, and a draft law on data protection[41] that would complement the related Omani laws. It also adopted the e-transactions law n°69/2008 which includes provisions on data protection, in agreement with the UN model laws on e-commerce and digital signatures. In fact, article 43, of chapter VII, "Personal Data Protection", stipulates that any data may not be collected, processed or used for any purpose unless with the explicit approval of the person about whom the data are gathered. The law also establishes the confidentiality of the personal data (art. 44), the obligation of notifying the data owner, prior to any processing, of the procedures that must be followed to protect the personal data (art. 45), the right of the digital certificate holder to access and modify his/her personal data (art. 46), the right to object to the data processing (art. 47), and to choose not to process them in case such data would cause any harm to the persons (art. 48) and the conditions to be met during the transmission of such data outside the country (art. 49).

The Sultanate of Oman's Telecommunications Regulatory Authority enacted the decision n°13/2009 issuing the executive regulation on the protection of the confidentiality and privacy of the data in use, and under which the wired and wireless communication service

providers are obliged to comply with special regulations to protect the data though there is no explicit text referring specifically to the data protection.

It is also worth mentioning the IT crime fighting law promulgated by royal decree n°12/2011 (official gazette n°929 dated February 6, 2011), chapter 2 of which is entitled: "transgression of the safety, secrecy and availability of digital data and information and computer systems" and containing 8 articles. This chapter incriminates the access to any website or electronic information system or information network or information means without a permit or the abuse of such permit, or the alteration, destruction or distortion of a website (articles 3, 7 and 9), particularly with relation to the medical file (article 5), or the access to government data or financial or economic confidential information (article 6), or the falsification of State e-documents (article 6), or the interception of the data flow (article 8).

The law incriminates as well the misuse of IT means (article 11), IT falsification, fraud or blackmail (articles 12 and 18), committing content crimes, specifically those against the ethics code (articles 14, 15 and 17), attack against private life (article 16), violation of religious beliefs and public order (article 19), e-terrorism (article 20), money laundering (article 21), human trafficking (article 22), trafficking of human organs (article 23), arms trafficking (article 24), drug or psychotropic trafficking (article 25), violation of intellectual or industrial property (article 26), trafficking of antiquities and artistic masterpieces (article 27) or illicit acquisition of financial cards (article 28).

In 2010, the Sultanate of Oman set up Oman's National Computer Emergency Readiness Team, "oCERT"[42], and hosts the ITU- Regional Cybersecurity Center for the Arab Region whose mission is to provide services and initiatives to the Arab region for better cybersecurity capabilities through coordination and ensure regional cooperation.

XVI. Syria

In 2004, the Syrian Arab Republic put in place a national strategy for information and communications technology. In 2009, Syria adopted the digital signature and network services law n°4/2009 which created the National Authority for Network Services[43], which, in turn, created "the Information Security Center" which issues periodical reports on the security alerts and evidences of security breaches, and provides information security services to corporations and technical support to public departments to prevent their website from being hacked or their own information and data from being published without authorization. Syria is setting up the Syrian Computer Emergency Response Team, "syCERT" as part of such center.

Then, it enacted Telecommunication law n°18/2010 where article 50 establishes the "privacy respect" principle. Under this law, the Syrian Telecommunications Regulatory Authority (SyTRA)[44] was set up. The law also provides for the creation of judicial police for the communications-related transgressions and crimes. In 2011, the Media law was issued by Legislative-Decree n°108 of August 8, 2011. This Law includes 106 articles divided into 8 chapters: definitions, basic principles, rights and obligations, National

Media Council, right of reply and correction, authorization and accreditation and their procedures, sanctions and criminal procedures, etc. There is also decree-law n°17/2012 to regulate communications over the Internet and combat cybercrime. This decree law regulates the network service providers' responsibilities and obligations and the identification of the network service provider on the Web and provides for the creation of a specialized judicial police. Moreover, the Ministry of Telecommunications and IT passed law n°290/2012 for the coordination of the illustrative and executive instructions of such decree.

In 2009-2010, the Ministry of Telecommunications and IT drew up a detailed strategy of the e-government that refers to the security of the public information systems and how to protect them[45]. In 2014, the Ministry of Telecommunications and IT issued the "National Information Security Policy" act which identified the scopes and requirements of work in this regard[46]. Here, it is worth noting that the Ministry has adopted a series of standards for the ICTs, including protection of ICTs[47].

Administratively, the importance of cloud computing is now recognized in public and private sectors, particularly as to wide disparity between the public institutions in classifying the necessary software for work.

XVII. State of Palestine

Palestine has recently recognized the importance of the use of cloud computing to keep up with the modern tendency and given its multiple advantages in developing the entire local community, particularly with respect to exchange of information, enhancement of the communications services, the education institutions and the business industry.

On the governmental level, the Ministry of Telecommunications and Information has recently set up the National Data Center, where the Ministry has shifted towards the virtual world, i.e. supplying services via the virtual technology and providing large capacities for government data storage and automatic backup, instead of the traditional service supply, where each service is provided on a separate server. The Ministry will use the Private Cloud Computing which serves the Palestinian Government, as it allows providing main or backup governmental services to other institutions without the need for data storage center in such institutions.

On the other hand, in the private sector, there are some private IT and telecommunications companies that use the private clouds, including SAS, PAS and ISAS, some of which work as service provider for international companies.

Palestine passed a series of laws and decisions, mainly:

- The departmental order n°20/2001 which created the Palestinian National Internet Naming Authority.
- The Palestinian Cabinet departmental order n°35/2004 on the right to access the Internet and the e-mail through the Government Computer Center.
- The Cabinet departmental order n°3/2004 on the prevention of sale and of marketing of communications services, information technology and express mail.

- The Cabinet departmental order n°26/2005 on the approval of public policies to use the computer and the Internet in the public institutions.
- The Cabinet departmental order n°74/2005 on the national strategy of the information technology and telecommunications (in this respect, the Ministry adopted the strategic plan of telecommunications sector for the years 2017-2022 as well as the national strategic plan of the e-government).
- The Cabinet departmental order n°65/2005 on the approval of the adoption of the E-Palestine initiative.
- Decision n°11/41/14/C.M./C.S. of February 19, 2013 on the adoption of the Palestinian Interoperability Framework "Zinnar" in all Palestinian ministries and institutions as a reference for digital exchange.
- Decision n°08/127/13/C.M./C.S. on the adoption of the information security policy document.
- Decision n°08/46/14/C.M./C.S. of March 12, 2013 on the formation of a Palestinian computer emergency response team (information security).
- Decision n°08/45/17/C.M./R.H. on the formation of the e-government permanent central team.
- Decision n°22/24/16/C.M./R.H. on the formation of the supreme ministerial committee.

In addition, other laws are being drafted, most importantly:

- The 2010 e-transactions law. The Cabinet departmental order n°01/22/13 was issued to form a ministerial committee for discussion of a draft law on e-transactions by the Council of Ministers on May 17, 2016 under decision n°02/103/17/C.M./R.H. and was transferred to the President of the Palestinian State for approval.
- The cybercrime law which was submitted for the Council of Ministers for a second review to adopt prior to its approval by the President of the State.
- Law on protection of personal data and information. On April 12, 2016, the Council of Ministers adopted departmental order n°09/98/17/C.M./R.H. for the year 2016 to form a committee delegated with the preparation of a draft law on the protection of personal data and information.

XVIII.Qatar

Since 2011, the cloud computing in Qatar (ictQATAR) was set up under the patronage of the Ministry of Transport and Communications, providing its services to the different State departments. A dedicated State cloud is being built to make the State institutions more competent and skillful, cut the investment cost, and enable the cloud computing environment by putting in place the necessary policies, such as the law on the data privacy and protection. Moreover, Qatar is teaming up with the innovative cloud service providers to meet the needs of the small and medium-sized enterprises.

At the legislative level, there are a good number of effective laws and initiatives aimed at creating a legislative and regulatory framework for the cloud computing in Qatar. The Qatar Constitution of 2003 included in article 37 thereof the EC directives of 1995

stipulating that the individual's privacy is sacred and no one is allowed to invade such privacy, unless according to the law and to the ways provided therein.

Qatar also enacted the anti-cybercrime[48] law n°14 of 2014, which incriminates the violation of the information systems, software and networks and websites (2, 3 and 4), the content crimes (5-9), the electronic falsification and fraud (10-11), the online card crimes (12-12) and the violation of the intellectual property rights (13-13). The law determines as well the obligations of the service providers (article 21) and of the State bodies (articles 22).

It also provides for the investigation procedures to follow and the evidence (articles 14-20), the mechanism of the international cooperation in terms of common rules (articles 23-29), the mutual legal assistance (articles 30- 38) and the extradition (articles 39-43).

There is also the Qatari telecommunications law n°34/2006 which requires the communication service providers that use the wired and wireless communications networks and their related systems to respect the clients' privacy and taking the responsibility of protecting the data and with a view to control the marketing communications. This is in addition to the e-transactions and e-commerce law n°16/2010 (August 19, 2010) which promulgates additional provisions related to personal data protection.

Qatar Financial Center (QFC)[49] has elaborated special rules on the protection of its own data and lists[50]. However, such rules only apply to the activities of this center and the banking services or the transfers made from the center outwards and for statistical purposes only (in addition to Dubai Financial Center).

There is also a data privacy draft law which is yet to earn approval, and which has been amended to include the obligation of keeping confidential the personal data of individuals and corporations. It would also impose high fines for the disclosure of any financial or non-financial information about the clients without their approval, which helps guarantee the security and protection of the data hosted by the local providers.

As far as the law enforcement agencies are concerned, Qatar set up authorities that cooperate to ensure web security and confidentiality, most importantly, Qatar Computer Emergency Response Team (Q-CERT)[51] which plays a preventive role in identifying the major threats to the digital domain and eliminating them to prevent any harm that may be caused to individuals. There is also the Cybercrime Combating Center at the Qatar Ministry of Defense whose mission is to detect such crimes and enforce the laws and regulations issued by the government against the violators.

In June 2014, Qatar laid out the Cloud Computing Security Policy for the State Institutions to give an overview of the challenges this computing presents in terms of security and privacy, discuss the technological threats and risks and how to protect the

cloud environments and offer the necessary vision and ideas to help the decision-makers in the ICT industry to take studied and practical decisions.

Moreover, Qatar elaborated the directives on the best practices in cloud computing which consist of assessing the readiness of the requirements of such services, laying out a national strategy, discussing the successful and failed areas, determining the information that can be saved on the clouds and those that cannot, and ensuring the performance guarantees and the availability of the data by the service providers and many other awareness-raising directives.

In May 2014, the State of Qatar adopted the National Cyber Security Strategy which promotes the concept of cyber security within the State and focuses on five important goals (protection of the infrastructure of the national critical vital information, response to, resolution of and recovery from electronic accidents and attacks, development of the legal and regulatory framework for the promotion of the cyberspace safety and vitality, promotion of the cyber security culture and development and forging of national skills). It also encourages private projects and initiatives in the information security field for the new technologies such as cloud computing and the new mobile applications and application of the smart grid technology in the important information structures.

Qatar Computing Research Institute focuses on three research themes: next generation cloud computing infrastructure, distributed algorithms to cover tremendous amounts of data, and cloud computing services and applications. The Institute endeavors to enhance the wireless display protocols that would be used with the cloud environments, create the next generation of media services based on the cloud computing, design data-centers that can operate in desert environment and the cloud-operated operation activities and understand the environmental impact on the cloud computing within the data-center environment.

XIX. Lebanon

At the legislative level, the draft law, ECOMLEB, prepared by the Lebanese Ministry of Economy and Trade, has adopted a large-scale term, the Personal Data, inspired by the French law of 2004. Moreover, a new draft law on the electronic transactions and the personal data has been also prepared based on the French laws and the European directives and in agreement with the other modern international tendencies in this area. Lebanon has already passed law n°140 of October 27, 1999 on protection of the right to confidential phone conversations.

In the same context, Lebanon has been collaborating with the ITU through:

- Participation in the Study Group 17 meetings of the Telecommunication Standardization Sector which ensure the coordination of work with regard to cyber security in all ITU-T study groups.

- Suggestion of contributions in the SG17 which is currently working on the cyber security, the security management, the engineering of the security and the framework, the fighting of e-mail spam, the identity management, the protection of personal data, the apps and cloud computing security.

- Follow-up and contribution in Q22_1/1 in the ITU-D Study Group 1 entitled "the Best Practices to Promote the Culture of the Cyber security."

In 2012, the Telecommunications Regulatory Authority (TRA) laid out a local plan to protect and maintain the security of the cyberspace in Lebanon, while conducting a thorough study of the necessary measures to protect the national communications networks against piracy. In July 2015, the Lebanese Ministry of Telecommunications launched the Vision of Digital Communications for 2020[52].

There are also many questions still currently unresolved in Lebanon, mainly: What about the sovereignty over the data? Where the data is supposed to be stored? Who would own such governmental cloud? What law would apply thereto? How committed the cloud computing service providers are not to transmit the crucial data outside the country, particularly those concerning the national security and the Lebanese sovereignty? Would there be one or more clouds? Such issues have not been resolved yet, however, governmental committees were set up to discuss such steps.

Practically, Microsoft in Lebanon provides public and private cloud solutions, to meet the needs of its clients, irrespective of how the Lebanese Ministries embrace the cloud computing. However, the governmental authorities must be aware of its importance and of its mode of use. Though what is even more important is to enact a law on the e-transactions and the cybercrimes in Lebanon. In fact, there is a number of companies that offer cloud-hosting services in Lebanon and work with small and medium-sized companies that lack functional capacities and prefer that all technological services be provided through a public cloud. Generally, there is a database that needs to have more privacy and must stay within the country such as bank secrecy which requires the banks to keep their information inside Lebanon.

Lebanon also suffers from the lack of specialized legislations and of procedural regulations, as well as the lack of specialized courts, of a CIRT (although there are attempts to establish one) and of conduct rules, as well as from the inadequate awareness-raising campaigns and training sessions for the judges, the judicial staff and the public opinion.

XX. Libya

Recently, more precisely in November 2015, Libya launched LCNA, the first Libyan cloud computing-based news agency. It uses a cloud service on servers located outside the country. In last September, the State launched the New Digital System for Libyan Students which uses the cloud computing techniques. From its part, the Ministry of Telecommunications and Information Technology has declared the "e-Libya initiative"[53]

that lays the infrastructure of digital Libya and includes e-services: e-networks, e-systems, shared data, cyber-security and other foundations. One of the strategies is also to build and develop a central data-center to provide the shared technical services and take advantage of the cloud computing, as well as to put in place the laws, regulations, policies and digital governance to ensure transparency and support the digital systems.

At the legislative level, no law has been enacted by the Libyan legislation authority with respect to the e-transactions, or the telecommunications or the cybercrimes. In fact, as far as the e-transaction issue is concerned, the latter only introduced one article into the bank law that dealt with reserve with the reliability of the electronic evidence in proving one kind of transactions, i.e. banking transactions. Currently, some parties are preparing two draft laws to regulate the e-transactions and fight cybercrimes[54].

XXI. Egypt

The new Egyptian Constitution has introduced some legal principles on the use of information and communications technologies. Article 31 thereof stipulates that the cyberspace security is an integral part of the economic system and national security. As for article 57, it enshrines the personal privacy, and the non-violation of postal correspondences, electronic mails and phone conversations. Egypt is committed to the protection of the citizens while they use public communication means in all its forms.

The Ministry of Communications and Information Technology of Egypt attaches great importance to the cloud computing, the data-centers, the integral solutions, and Web 2.0 in order to encourage and foster the development of the cloud computing and its uses, as well as the related techniques in the government. Several memorandums of understanding were signed in this regard with different countries (e.g. Germany, Malaysia, Singapore, etc.) for expertise exchange to ensure the readiness of the Egyptian staff to catch up with this new industry.

Since 2012, the MCIT also organized several workshops and held a number of training sessions for judges and judicial staff. Moreover, it initiated the Technology Day on Cloud Computing and the Weekend on Cloud Computing to raise awareness about its importance and highlight the international directives and the best practices.

At the legislative level, the most important law is law n°10 of 2003 (on regulation of communications)[55] which regulates the lists and services of the communications networks, thus legitimating the vital role the Internet service providers play.

In August 2011, the Egyptian Ministry of Communications and Information Technology formed a committee of experts in different legal and technical domains to elaborate new relevant draft laws such as:

- The “freedom of information” draft law which deals, among others, with the regulation of the data and information availability and the personal data protection, the incrimination of their use for purposes other than those for which they were disclosed. The freedom of information draft law sought to set up legal controls and

regulations on data and information disclosure, while establishing the right to privacy and public freedoms.
- The "cyberspace security" draft law aimed at protecting the cyberspace with all its content against any external assault.

At the judicial level, by virtue of law n°120 of 2008, the economic courts were set up to adjudge the criminal cases related to economic and investment activities, and those related to the information and communications technology. Judges and public prosecutors received several trainings in cooperation with international organizations and multi-national companies specialized in ICTs. A dedicated department was also established within the Egyptian Ministry of Interior by ministerial order n°327 of 2005 to fight the web-and networks-based crimes.

In 2010, Egypt established the Egyptian Computer Emergency Response Team, EG-CERT[56]. Moreover, there is a top-level management within the National Telecommunication Regulatory Authority (NTRA)[57], which provides the technical expertise in evidence examination in cybercrimes. The NTRA aims at achieving important breakthroughs in the ICT sector, which helps in supporting the capacities and advancing the sector. It also aims at acting as influential arbitrator that maintains balance between the State, the ICT industry and the users.

XXII. Mauritania

In 2015, Huawei has launched a new generation of storage and cloud computing solutions in Gitex in Mauritania.

Legislatively, the Mauritanian legislation authority has never issued any law on the e-transactions or the communications and information technology or cybercrimes. However, there is a draft law under preparation on "the legal framework of the Mauritanian information community" which stipulates the data protection, creation of an authority that guarantees such protection, and the non-transfer of data to other countries save some exceptional cases. Mauritania is considering introducing the electronic payment system for the banks' financial transactions.

Since 2014, the Mauritanian government started to take interest in the "cybersecurity" and enhance its capacities in this field seeking to protect the information systems and data of the State private and individual institutions.

The following table lists the States that have CERTs in the Arab region:

Name of the State	Name of CERTs or other Authority	Website	Year of establishment
Jordan	Working on the creation of the computer emergency response team, The National Information Technology Center, The National Center for Security and Crisis Management (2015)	---------	---------
United Arab Emirates (UAE)	aeCERT	www.aecert.aw	2008
Bahrain	Creation of the Communications Regulation	www.bix.bh	

	Authority, Creation of Bahrain Internet Exchange, Regulation of the Central Informatics Organization, Supreme Committee for Information Technology		
Algeria	Non-existent	---------	---------
Kingdom of Saudi Arabia (KSA)	saCERT	www.cert.gov.sa	
Sudan	sudanCERT	www.cert.sd	2010
Somalia	Non-existent	---------	---------
Iraq	Non-existent	---------	---------
Kuwait	Working on the creation of the computer emergency response team, CITRA, Kuwait Information Network	https://www.cait.gov.kw/National-Projects/Kuwait-Information-Network.aspx	
Morocco	The National Control Committee for the Protection of Personal Data	www.cndp.ma	---------
Yemen	The National Center for Information (1995)	http://www.yemen-ic.info	---------
Tunisia	tuCERT	www.tuncert.ansi.tn	2007
Comoros	The National Authority for Regulation of Information Technology and Communications	http://www.anrtic.km/	2009
Djibouti	Non-existent	---------	---------
Sultanate of Oman	oCERT. Creation of the Telecommunications Regulatory Authority	www.cert.gov.om	
Syria	Working on the creation of the computer emergency response team	---------	Underway
Palestine	Non-existent	---------	---------
Qatar	CERT.	www.qcert.org	2005
Lebanon	The Telecommunications Regulatory Authority, TRA	http://www.tra.gov.lb/	
Libya	Non-existent	---------	---------
Egypt	EG-CERT The National Telecommunications Regulatory Authority (NTRA)	www.egcert.eg http://www.ntra.gov.eg/arabic/main.asp	2010
Mauritania	Non-existent	---------	---------

Part II: Best Practices of the Cloud Computing Legislative Framework: Comparative Study

The legislative initiatives have been launched by several countries and by the international and regional organizations, to ensure the legal security of the databases, and prevent their transmission, notably the United Nations, the International Telecommunication Union, the World Intellectual Property Organization and the European Council.

Clause I: United Nations, ITU and Cloud Computing:

The Study Group 17 of the ITU Telecommunication Standardization Sector has been studying the security of the cloud computing since April 2010, setting directives and conditions in several domains, including the identity management[58].

In 2013, the Union issued a report on the "Trends in Telecommunication Reform 2013, Transnational Aspects of Regulation in a Networked Society" which includes a chapter titled "The **Cloud: Data Protection and Privacy Whose Is It Anyway?**" discussing the cloud computing services, its social and economic benefits, the current regulatory rules applied thereto, in terms of data protection and privacy. The report recommends that a coherent domestic and international policies and regulation to be set up for the uptake of global cloud services to achieve a balance between the needs, the commercial opportunities, the technological situation, and the reasonable expectations by citizens, with respect to privacy, in a global, digital and ecological system.

In general, ITU has been making diligent efforts to achieve cybersecurity. In this respect, the Union issued the 2007 Cybersecurity Guide for Developing Countries, as well as lots of programs and action plans to bring the necessary standards to the cloud computing services field and enhance the use of the best practices in order to guarantee their security. Several relevant organizations were formed, most importantly, the Cloud Security Alliance (SCA) which is being designing a protocol to secure the cloud computing to promote the best practices in the industry and ensure transparency to the cloud computing users.

A reference must be made to the project launched by ITU in cooperation with ALECSO[59] under the umbrella of the Arab Network of Regulators (ARGENET) on the use of cloud computing in the Arab educational institutions in order to check the extent of adoption of this technology in educational and research institutions in the Arab countries and the proportion of its use, also to spread awareness of its advantages and benefits, particularly to serve education and learners, and support its use in the education and scientific research field in the Arab world.

The importance of this project is highlighted given the lack of well-defined digital development plans in the higher education institutions in the Arab countries. In fact, the education sector is a major beneficiary from the cloud computing services. Therefore, it is

important to develop the digital environment in the education sector and the educational institutions, particularly the higher education in the Arab countries, this will provide the university professors and teachers with tools of creativity and innovation, and let the students access to enormous resources, namely computer applications, foreign and local libraries and other programs at low or even free cost, and for the exchange of research and studies.

The UN General Assembly has taken into consideration some principles[60] the States in question make sure to include in their laws such as the legitimacy and the integrity of all personal data[61].

Moreover, the Organization for Economic Cooperation and Development (OECD) recommended the member States to comply with the data privacy protection guide for natural persons, with respect to the date which are manually or electronically processed in public and private sectors. The guide contains some basic principles[62].

The ESCWA directive 24 stipulates that the personal data may not be transferred to a foreign country unless this country secures a certain level of legal protection. Directive 25 thereof highlights the exceptions, including the consent of the owner on such transfer or the transfer of the data is necessary for certain reasons[63].

Clause II: The European Union's Leading Role

The European directive 46/95/EC of October 24, 1995, on the protection of the natural persons as to the processing and free circulation of personal data, constituted the first European initiative aimed at protecting the personal data, and which is in accordance with the European policy on the protection of human rights. The application of such directive was only limited to the EU countries.

According to article 25 of the above directive, it is forbidden to exchange data with non-EU countries[64] that do not ensure a protection equal to that of the EU States[65]. The European Commission is the reference authority to decide if the other State is ensuring the same protection or not. So far, few non-EU countries ensure the same protection: Canada, Argentine, Uruguay, New Zealand, Switzerland, Andorra, Jersey, Israel, Guernsey islands and Isle of Man.

In the same context, a Safe Harbor Agreement[66] was signed with the United States in 2000[67], requiring the US companies to comply with a number of principles that forbid any violation of personal data. This includes the obligation to inform and identify of the purpose of the collection, use and transmission of data to third parties; the right to access and make corrections to the extracted data, as well as the information security, the data

authenticity, the creation of mechanisms for objection and execution, the consideration of the victims' complaints and the estimation of the damages.

It is important to refer to the US-EU agreement (Accord de Washington) signed in 2004[68] which requires the Union to make sure the airlines carriers provide all necessary information for the aviation safety. Under this agreement, the United States must offer guarantees to provide the same data protection as that determined by the European Union. In 2012, both parties signed another safe harbor agreement[69] on the transmission and analysis of the passengers' data to be restricted only to fight terrorism, drug trafficking, human trafficking and other crimes, and keep these data for a period of ten years, within the framework of legal, regulatory and security cooperation. In fact, this agreement provides security only to the big companies.

Judicially, on October 6, 2015, the European Union's Supreme Court declared that the safe harbor agreement[70] for data exchange with the United States is invalid following the Facebook case, considering that the said company should not simply deliver the users' data to the US authorities. According to that court, the reason for such invalidation is that Facebook and other technology companies, such as Google and Amazon, had exploited such agreement and transferred the users' data in large amounts to its own computers in the United States, where they would have been kept. This judgment will absolutely have an impact on any US company dealing with EU data including Twitter, Microsoft, Yahoo and Google.

Concerning the EU consumers contracted with the cloud computing providers that not governed by the safe harbor agreement, must be subject to the EU legislations on the transfer of personal data. Amazon, for example, created a European website for cloud computing that assures the consumers that their data will not be transferred across the borders so as to constitute a breach of the EC directive.

Here, the EC directive dated October 24, 1995, on the protection of people concerning the treatment of personal data, and the freedom of transferring data, including medical and genetic data[71].

In 2010, the European Commission issued model clause to comply with when exporting some data outside the European Union (European Commission - 2010/87/EU - publication on February 5, 2010)[72].

In the same context, the 2002 European directive[73] was directed at the public and private communication network providers. Under this directive, the personal data must be accessed by virtue of a personal mandate for the legally authorized purposes, or must be protected, during storage or transmission, against illegal or incidental damage, or loss, or incidental change, and against illegal or unauthorized treatment, access or disclosure.

A reference must also be made to 2001 Budapest Convention on Cybercrime[74] which provides for the State's commitment to keep, wherever a cybercrime is committed, the

data related to the telecommunication movement and disclose them to the State requesting such data.

It is also important to make reference to the regulatory framework of the Council of Europe's action, dated November 27, 2008, on personal data protection[75] in the area of judicial and security cooperation with respect to the security and military affairs-related data, exchanged between the Union States.

Moreover, the leaders of industrial and commercial sectors in Europe approached the European Commission to find the appropriate legislative framework for the cloud computing services[76].

In 2009, the European Commission issued a code of conduct on the efficient consumption of energy by databases, setting up a series of voluntary measures such as achieving efficiency in the design and operation of databases[77]. On January 25, 2012, the European Commission published the modifications suggested to be brought to the EC directive on personal data protection[78] in an attempt to harmonize the legislative framework and all local laws on data protection within the Union. The suggested modifications include:

- To empower the national regulatory authorities to take measures against companies operating within the other member States in specific circumstances, with the right to impose fines up to €2M or, in some cases, 2% of the company's annual turnover.
- To expand the definition of personal data so as to cover any information in connection with the data holder, with the regulations stating as condition the explicit approval of the individual to allow the inaccessibility of the data.
- To apply the regulations beyond the European Union, so as to include the entire non EU States (which have personal data in connection with the EU citizens).
- The appropriate authorities in question must notify, without any unjustified delay, of any data breach within 24 hours of occurrence of such breach.
- The companies controlling the data must assess the impact of data protection and entrust officials with the task of protecting the data and alerting third parties to any breach.
- The individuals shall have a new right, i.e. "the right to be forgotten" in specific cases, and they are no more requested to pay a consideration to access their data.
- The international data transfer shall be governed by a more detailed regulatory framework that imposes guarantees to be applied. In addition, the authorities must conduct prior examinations to further restrict the ability of the companies controlling such data to invalidate such guarantees.

In May 2012, the European Parliament published a study determining the methods that policymakers must adopt to facilitate the cloud computing[79]. These methods include dealing with gaps related to legislations and enhancing the terms and conditions for all

users; addressing the fears and concerns of stakeholders related to security, encouraging the adoption of cloud computing in the public sector[80], and expanding research and development in this area.

Clause III: Western Local Legislations

The CSA Model Code provides for the personal data protection and digital documents[81]. The Canadian courts have also enacted a public law on the damages resulting from the privacy violation. In fact, no restrictions are imposed by the Canadian law on the international personal data transfer, but the disclosing party shall remain liable for such transfer.

In addition, the 1998 British law[82] on data protection authorizes the transfer of data abroad once the enterprises ensure that the information provided are well protected by the country to which they are transferred.

There is also the American Patriot Act[83] (passed following September 11, 2001 attacks) which authorizes the sharing of personal data of any individual suspected of being involved in terrorist acts or money laundering. The National Commission on Informatics and Liberty (CNIL) in France has published a directive on the legal processing of personal data[84] compelling the companies controlling the data to comply with the notification and cooperation conditions and to ensure personal data security[85], and in some cases, the prior approval of the authority is required concerning the data processing[86]. The US act also obliges all cloud storage service providers, headquartered in the United States, to make available all data stored in their servers to the US security authorities.

French Legislation: The French lawmaker passed act n°17/78[87] of January 6, 1978 on Data Protection Act (La loi informatique et Libertés) with regard to the digital processing of nominal data. This act was subjected to several amendments[88], the last of which under law n°801/2004[89] by virtue of which the EC directive of 1995 on personal data protection was adopted. In 1981, the act served as a model for the European Council Convention[90].

The act defines personal data as nominal information pertaining to a natural person whose identity is identified or may be directly or indirectly identified, excluding other data that may serve the same purpose. It is worth noting that the act, as amended in 2004[91], used a more comprehensive expression, namely "personal data". Thus, by expanding the definition, the French lawmaker has set new aspects more comprehensive of the personal data that require protection. However, the French jurisprudence has limited the jurisdiction of the French courts in terms of application with regard to the conflict of jurisdictions, if the damage, which occurred in the French territory, is neither prospective nor virtual[92]. In fact, there is contradiction in the French jurisdiction on the personal data protection between judgments supporting such protection[93] and others against[94].

The major amendments made to the French penal code of 1992 include that of law n°410/2012 dated March 27, 2012, and the new modification by the law n°912/2015 on July 24, 2015 (article 4)[95] which added new sanctions to articles 323/1, 323/2 and 323/3 on cybercrime targeting personal data[96].

Under the French code of 1998, databases are protected for 15 years and may not be reused, whether partially or in whole, by way of distribution, reproduction, renting or transfer via Internet. The transfer from the database content, in part or in whole, is totally forbidden whenever the access or the transfer is permanent or temporary on a support by any way or in any form. There is also the French decree n°632/2008[97] (EDVIGE) which aims at collecting and analyzing the data of natural and legal persons.

Clause IV Legal Standards, Regulations and Legal Suggestions

Practically, the major foreign companies still control the Arab market in the cloud computing field. Companies like Microsoft, Amazon, Google, etc. are main providers of IAAS, and there is almost no competition in the Arab market between those companies. This poses risks of monopolization and unfair competition by those expert companies due to the lack of regulations governing the industry or due to some existing de-facto standard. The public sector is the third source of security standards in cloud computing. In fact, public authorities in some countries have adopted cloud computing solutions provided by the private sector.

From a legal perspective, what are these international companies?

If the current global economic system is rightly described as the globalization age, it might be better described it as the age of multinationals corporations which are considered as the backbone of globalization. These multinational corporations form a business constituted of subsidiaries which are linked to the main office in the home country by legal relations, follow a general economic strategy (guidance, planning, organization, oversight, control, etc.) and make investments in multiple geographic locations. They also have an immaterial capital in form of technical know-how, patents, trade relations and local and international reputation, in addition to marketing tools and techniques.

While these companies do not enjoy an international legal personality like States and international organizations, they play an important role in international relations as international pressure groups at the political, syndicate, religious, financial and economic levels. They also have financial resources and their activities go beyond the limits and the budget of one State.

On another hand, the data protection is not only one aspect of the right to privacy[98], but also one of the citizen's basic rights to protect such data against violations from third

parties, and even against the arbitrary intervention from the government or from the foreign companies that break such right through the services they provide. It is worth to mention the data espionage[99] and the catastrophic cyberattacks such as cyberwar and cyberterrorism. This is why the decision-makers in the Great Powers view the cyber defense and cybersecurity as a top military priority and a priority in their national and defensive policies.

2. Contractual Aspect of the Cloud Computing Legislative Framework: Suggestions and Standards:

The main challenges raised by the modern technological tendencies of cloud computing are the contractual and administrative challenges in the Arab States, namely regarding the preparation of contracts and agreements which ensure service safety and security and data protection when in fact Arab jurists lack the expertise and experience in that regard, and have no model contracts to be followed.

Thus the contractual aspect of cloud computing includes the category of the contract, its terms and conditions and the appropriate mechanisms to deal with the legal and security issues and effects of the services provided by such computing. The two parties of the security issues in cloud computing are the client and the service provider who must ensure a good infrastructure and safe storage particularly if its services are paid for.

The following table shows the challenges of the contractual aspect in the cloud computing contracts:

Contractual Aspect Challenges:
• Lack of model laws • Lack of model contracts • Lack of Arab expertise or experience • No constitutional or legal protection for personal data • No Arab law incriminates or penalizes the business of multinationals • There are only local or international rules for the conduct of moral value

The pre-contract phase is important to negotiate and determine the conditions and content of the service subscription contracts, the technical-content contracts, the contracts of the parties in connection with the websites, or the users' contracts, including the service request contracts and the paid-for and free-of-charge services contracts; in order to ensure the necessary compensation in case of breach of the contract terms by any party; to follow up the payments made to the service providers and the Internet service outage for environmental or administrative reasons, or to decode the passwords or service instruction keys.

The following table shows the challenges of the pre-contract phase:

Pre-contract Phase:
• to negotiate • to determine the legal and technical conditions (general, detailed and marginal) • the civil and criminal responsibility resulting from the violation of the contract and the amount of damages

As for the signature of the contract, it is one of the most important and critical phases due to the main problems[100] raised by cloud computing services and applications, particularly with regard to the liability in case of termination of the contract and the obligation of the service provider to give the data back to the client (whether States or individuals) and not to keep them and use them against him or handed him over a photocopy, not the original.

The following table shows the challenges of the contract signing phase:

Contract Signing Phase
• Type of contract (contract of adhesion/aleatory contract) • a non-negotiable and non-modifiable contract • Conflict of laws and determination of the applicable law

Therefore, the client must make diligent efforts upon the signature of the contract with the service providers, for most often, the standard form contract (adherence contract)[101] is imposed: it is a non-negotiable and non-modifiable contract where the terms and conditions are set by one party (the powerful party), while the other party has no ability to negotiate favorable terms (for example but not limited to, the contracts signed between small companies and Google), in light of the absence of the laws relating to cloud computing[102]; and in light of the conflict of laws that would apply to any dispute or lawsuit (whether it is a positive or negative conflict). In France, the French law applies only to that type of lawsuits, if the party in charge of the data processing resided in France or in case the data were processed on the French territory.

Suggestions, Standards and Horizons:	
1. Data Security: • strong password • not sharing all data, files and folders • An antivirus software • Regular backup of all databases.	**2. Client precautions of**: • Virtual machine • Malware and viruses • Poorly secured cloud computing • Challenges of the management of big data centers.
The contract clauses: • Possible access to information	

- Data storage, processing and transmission procedures
- Client ownership of the database
- Term and end of the contract
- The force majeure consequences
- The guaranteed payment for the services provided
- Receipt of the original copy upon the contract expiry
- Destruction of any spare copies

- **Data Security**: There are other issues, including what the service providers have realized, i.e. that while some users do not care about what happens behind the websites scenes, some of them (mostly professional or curious people) might have several reasons to find out what goes on in the backstage of websites. While some companies and websites endeavor to develop their services to meet the requirements of their clients and maintain them and to manifest their competitiveness among their peers, some technology fans always want to discover the latest developments in the digital world even in an illegitimate or unauthorized way (by electronic piracy). The studies show an important disparity in terms of willingness to use cloud computing between the developed countries (with Japan at the vanguard) and the developing countries[103].

There are multiple reasons behind such disparity: lots of concerns and cautions are associated with this service in the Arab countries, most importantly the information security standards, the poor infrastructure, the category of adhesion contracts, the computing applications in some of these countries, their cost and the necessary arrangements and controls, the extent of cooperation with the competent international authorities and the specialized giant companies, the internet outage, their poor services and the environmental concerns.

However, the user must safely use the service by inserting a strong password to authenticate the cloud account, not sharing all data, files and folders and other links with others, installing an antivirus software, and making sure to have regular backup of all his/her databases.

Therefore, the client must make sure to include in the contract clauses to cover the following points: hacking of virtual machine like any physical machine, hacking of software by malware and viruses, security management of the cloud computing layers (data centers, network, machines, operating system, middleware, applications, user…), challenges of the management of big data centers and service centers, flexibility and accuracy, optimal use of resources, scalability, effectiveness, competence and reliability (the client's confidence in the service and its continuity). The contract must also include clauses that highlight the possible access of information and the measures to be taken to save, process and transfer the data, and most importantly an explicit, clear clause proving

the ownership by the client of the database, and indicating the contract duration, the force majeure consequences, the guaranteed payment of the services provided, the contract expiry, the handover of the original copies and the destruction of all other backup copies.

- **Obligation of Protection**: At the security level, the companies, and even the States, are unable to protect their information against the security breaches and attacks which are more and more complicated and difficult to detect, which requires regulations to be set up in order to fill any security gaps and provide technical protection which is proportionate to the size of such database, yet logistic protection of the local physical buildings containing such data. The user is also required to verify the service provider's reputation, its registered address, its local and international branches, its legal status (at least regarding its non-filing of bankruptcy) and the locations of its servers around the world, at least those in the United States and which are obliged to make available all their data to the US authorities. The user must also verify the quality of the technical support, the easy use and recovery and a high level of data security. He must most importantly make sure to read the conditions of use included in the contract, particularly those affixed in the margins that contain basis and accurate exceptions.

Thus the cloud computing service providers must be highly able to contain and recover the data in case of service failure. It is worth noting that the majority of the service providers protect the data by encrypting them, and such data may only be decrypted when the user inserts his/her password. This is why the data must be protected and the client must check how good is his/her connection to the Internet, and make sure that his/her account is not hacked, and of the user's real identity, and to well store the data, while the service providers must offer data processing and software tools to develop any programming code to assist the user in preventing any data leak and safeguard his/her rights and privacy.

3. National Sovereignty, Cloud Computing Security and Cross-border Security Challenges:

In the same context, it is important to say that the cross-border crimes and terrorism[104] make it important for the States to cooperate in the exchange of the personal data and information of people suspected[105], or pursued or convicted in cross-border organized crimes and terrorist crimes[106] that undermine the world security and peace and make the cross-border security as a top priority in the crime fight or prevention policy[107]. This is why it is important to exchange the information and well examine the passports, the visas, the traveler's record, the trip details, the airline or the travel agency, the ticket price, the

method of payment, the destination, the accommodation, the hotel[108], etc., which made it possible to expand the scope of access and sharing of personal data.

National Sovereignty and Cross-border Security Challenges:
• The importance of sharing of personal data • Sovereignty over database • Sensitive data: security, financial and banking information • Laws to be applied • Violation of the State sovereignty. • Intellectual property rights • Data security and privacy • Lack of guarantees against non violation of rights, laws and sovereignty

Several questions concerning the national sovereignty are raised. Not all the databases require the same level of protection: There are sensitive data concerning the national security[109] and the economic security (bank secrecy). These major challenges include the sovereignty over the database, the law to be applied and the location of information and data[110], which provokes concerns about security breaches and digital espionage and their consequences such as the violation of the national sovereignty and other moral and physical damages.

In most countries, the database center is subject to the law and the sovereignty of the host country. And the question is: if a judicial order was issued by a local court, would the service providers execute it? In fact, whenever stored and processed, the data turn from mere information to a database of high financial and commercial value. On the same note, the storage of the user's data with the service provider arouses fears that such data to be accessed or hacked by specific parties, the poor protection of the intellectual property right, the data security and privacy, and the possible access by third parties of their information and data amidst lack of guarantees of the non-infringement of such rights.

- **Management of Big Data**:

Many issues may be added in this context especially with respect to the encryption techniques on the cloud, the encryption mechanisms, the limits and disadvantages of the techniques, the multiplicity of users and the possible loss of control over the data. The question is what authority is qualified to assess the mistakes of the cloud computing applications, particularly the big data which became so large and complex that it is difficult to use local or traditional data processing applications which depend on one database. For example, these major companies have massive pools of private data and personal memories such as Google Photos where such data are only processed through that service, and thousands tons of photos are stored on the cloud computing system.

Management of Big Data:	
• Massive pools of private data and personal memories, • The encryption mechanisms, • The limits and disadvantages	• Loss of control over the data • Client awareness • Risk assessment, inquiry regulations and measure control

of the techniques, • The multiplicity of users	• Response to security accidents and technical emergencies

According to the US National Science Foundation, the spread of cloud computing in natural and social environments result in unparalleled inconsistent data in terms of size and complication. The challenge is for the client to be aware about the management and processing of these data, the reliability of the stored information, the risk assessment, the measure control and inquiry systems, and the response to security incidents and technological urgencies.

- **Consumer Protection**: The issues that arise in this regard include the rights of users and of those using Internet environment, particularly protection of the consumer in cyberspace, whether it is an individual or a corporation, especially given the near absence of appropriate Arab laws, the nature of adhesion contracts, the deceptive advertisements[111], and the difference between the professional consumer and the consumer who has no experience in e-commerce and other e-transactions[112]. Therefore, the jurists in the Arab world must consider the modern legal and administrative requirements of the cloud computing particularly under the pressure of legal threats given the nature of the cloud computing services compared to the traditional services.

Consumer Protection: • Users' rights • The nature of adhesion contracts, • The deceptive advertisements, • Modern legal and administrative requirements • "Trade of personal data"

According to a report issued by ITU, entitled "Trends in Telecommunication Reform for 2013", there is an increasing challenge facing the policy makers in making a balance between the trade need and the wish of the individuals in the free flow of information with previous knowledge and effective control by the individuals of their personal information[113].

The personal data has now an economic value, and lately a new phenomenon called "trade of personal data" has been appeared. Specialized advertisers[114] are taking advantage of the personal data by exploiting the data of consumers, employees and colleagues, friends' list, the images, the events, the traffic data, the IP addresses, the log files, the GPS data, the digital records, etc., in order to process them and post them later via specialized websites for promotive purposes such as e-marketing, and commercial purposes such as e-commerce without their approval[115]. These data are important for the service providers since they are a basic property that fosters their business models[116] and help them make a decision, reinforce their ability to innovate, achieve competitiveness

and increase productivity. The personal information is considered among the company's movable assets in case of their sale in whole or in part.

4. <u>Regional Coordination and Cooperation between Arab States</u>:

Constitutionally speaking, there is no constitution in the Arab region that provides for the right of access to information, or regulates by any of the aspects of protecting the privacy of information. No Arabic Constitution has mentioned the personal data or e-processing, or included a restriction of the data collection, storage and use by the public authorities.

Measures must be taken between Arab States:
• Legal, judicial and security cooperation between Arab States • Institutional and administrative cooperation between Arab States • Enhancement of the transparency of corporate behavior and financial reports • To conduct investigations and prosecutions • To strengthen the accountability of the companies' officials • Partnership between law enforcement systems and the private sector • Contribution to the enactment of an international law to be enforced on the illegitimate acts committed by multinationals.

At the legal level, so far, no international or Arab law incriminates or penalizes the business of multinationals corporations; there are only local laws and rules of conduct with moral value, without being compulsory. Therefore, the following measures must be taken: the need for legal cooperation between Arab countries; continue to enforce the laws strictly in order to increase the level of transparency of corporate behavior and financial reports; the need to conduct investigations and prosecutions; strengthen the accountability of the companies' officials; promote partnership between law enforcement and the private sector. Yet the most important, an international law, in form of international conventions, must be enacted with regard to illegitimate acts committed by these companies.

At the judicial level, the local Arab courts are currently aware of the importance of data protection management services and the approval of digital evidence, albeit the legal challenges they face concerning the reliability and authenticity of the digital proof. Consequently, the client must be aware of how much liable the service provider is in case of legal proceedings, arbitration or mediation. The local courts will certainly have to deal with traditional cases with digital proof in case of claim for data leak from their systems. So it depends whether there is a legal contract or not, and whether the ignorant may benefit from the fact that he/she is unaware of the laws, or the non-use of the necessary protection standards, or the non-compliance with such standards, in violation of the protection of the consumer and the network user, in addition to other conditions that must be met for the damage to be established as a basis to claim compensation.

5. <u>Arab Safe Harbor Agreement</u>:

Since the Arab countries do not effectively cooperate on the cybersecurity and the cloud computing services, therefore, the study suggests the importance of signing an Arab Safe Harbor Agreement with the following items:

- To set common standards and determine the cross-border information flow requirements with the right protection of security and privacy to be ensured;
- To achieve a regulatory progress to deal with the data protection and the security concerns;
- To make sure that the Arab countries are abreast of the best regulatory practices;
- To thoroughly prepare the cloud computing outsourcing contracts and include in such contracts effective sections about the data safety, particularly the national security-related data;
- To make sure that the cloud computing contracts contain regulatory conditions and include strict clauses concerning the data security, processing and protection;
- To set up data centers in the Arab countries and in every country separately to minimize the bandwidth costs and accelerate the accessibility;
- To ensure the ecological safety of data centers;
- To establish an Arab public authority to watch over the good application of the terms of such agreement;
- To include an arbitrary clause to settle conflicts and disputes through arbitration, mediation or resorting to local courts;
- To include a penal clause to apply it in case of breach by either party of the agreement terms, particularly concerning the transfer of data abroad without the consent of the client, or the non-recovery of same or the recovery of an unoriginal copy;
- To ensure cross-border standardization and regulation by taking part in the cloud computing standardizations initiatives;
- To abide by a number of principles, most importantly that of State sovereignty, equality between States, and its right to take advantage of the cloud computing services and to ensure the competitiveness of their companies;
- To set up national arbitration bodies specialized in cloud computing and preventive consulting services.

<u>Arab Safe Harbor Agreement</u>:	
1. To set common standards 2. To determine the requirements of cross-border information with the right protection for security and privacy 3. Protection of data and security measures 4. The best regulatory practices 5. Meticulous preparation of cloud computing outsourcing contracts 6. Data security, processing and protection	7. Arab Data centers 8. The ecological safety 9. Arab public authority 10. An arbitrary clause; national arbitration bodies 11. A penal clause 12. Cross-border standardization **13.** Principles relating to the State sovereignty

Conclusion and Proposals

To conclude, the cloud computing is considered as the next stage of technology or the next level of Internet development. It is more about new services than about new technologies, and like any production of the modern technology, the cloud computing system consists of two parts: the benefits and the challenges. In fact, the system has several advantages such as facilitation of participation, increase of revenues, expanding of business, creation of new job opportunities; however, it creates challenges related to contracting, security, data privacy protection, national sovereignty and legislative and regulatory framework.

It seems that the modern age is based on the embodiment of the "network community", big data, mobile phones, social media, storage of huge files, which is a source of worry for States, experts and specialized organizations since it rises the cloud security incidents and creates more problems related to network and traditional applications and data storage, particularly loss, theft or transfer of data abroad, State sovereignty over the data ownership, fraud issues, encryption, piracy, security breaches, protection of clients and of users. In this context, many Arab States have launched projects and strategies to adopt the cloud computing techniques but in the absence of a legislative environment that determines the legislative, regulatory or executive frameworks and with no national legal, contractual or security strategy drafted, in addition to the lack of cooperation at the local or foreign level. Moreover, the telecommunications sector has particularly emerged as horizontal industry that intersects with all the main sectors of the State under a modern technological system with which traditional ways do not work.

In general, many Arab countries have not set up a comprehensive legislative, regulatory or executive structure for e-transaction, data protection, processing or transfer abroad, or fight against cybercrimes, and few of them have established telecommunication or emergency centers. So what about a legislative framework for the cloud computing? And how effective and consistent the Arab environment is with the digital environment? Maybe, few people are familiar with the term "cloud computing", and the ambiguity of the expression, in terms of the current and new emerging techniques it contains, makes it difficult to find one definition, which is essential to every legislative framework.

One also concludes that the reluctance of some Arab States and local companies to use the cloud computing applications is due to the fear of some people from the service interruption, on one hand, and the security in all its informational and legal forms, from the other hand. These companies need a permanently available infrastructure with no Internet disconnection as well as specialized technical and human experiences and high skills in IT field within the same company and in order to provide security and logistic protection to the data centers that contain cloud computing services against hacking and manipulation of the data contents therein.

The Arab States are recommended to set up their own IAAS services, for these States have the right to keep their data and information. By providing such services locally, there would be a better safety and support service and more flexible communication with clients and companies whether the data belong to individuals or to the private sector, or to the public departments and State institutions of those States, because any Arab country is likely to face a real threat to its national security.

In addition, the investment of the Arab States in the activation of cloud computing services would create lots of job opportunities for the Arab youth and they do not have to worry about the adoption of such services because even laptops suffer from security breaches.

Certainly, not all the information has the same level of sensitivity. For example, the national security-related information must be always under the State sovereignty or within the building of the Ministry concerned. Thus they need a special cloud protected by civil servants. However, some information, data and applications can be available on a public cloud. In fact, one of the important subjective and procedural challenges of the cloud computing control is the lack of internationally binding legislation (i.e. an international convention) covering all the States of the world, but most of the States have adopted the privacy and data protection and many of them regulate the international data flow as a mechanism to protect the privacy of individuals and to put in force the national policies.

Thus the proposals of this study are divided according to local and regional levels:

I- <u>Locally</u>

- **<u>Legislative Proposals</u>**
  - The importance of reviewing the applicable laws to know how much they contribute to an easy national and international use of the cloud computing services.
  - The participation of the public policy makers in the States in drawing up local policies that stress the importance of computing and of catching up with the technological development in consistence with the national priorities.
  - To update or develop the legislative environment, the suitable laws and regulations, the executive decrees and the practical decisions.
  - To enact laws on new taxes to be levied and to introduce the 4G band to all the regions.
- **<u>Executive Proposals</u>**
  - To enhance the administrative environment given the correlation between any local advance and the specialization of the bodies concerned and their ability to put laws into force and control the mechanisms.

- The contribution of the State to enable local companies to create an environment of technologies that allows them to compete at the regional and international levels (incentives such as exempt companies from some financial and fiscal obligations).
- To take advantage of the best practices and successful experiences at the international level, and to adopt the international standards and norms which increase the reliability of the cloud computing and ensure a supportive environment for integration in the digital economy in whole.
- The importance for the Arab States to benefit from the cloud computing services while taking into consideration the following points:

✓ Data protection: The client has the right to keep his/her information and prevent their leak. He should make sure that he/she is connected to Internet and should save his/her information in a safe and sound way, in addition to his/her right to resort to legal protection means in his/her country and to international standards set by the competent authorities.

✓ Identity Management System: To verify the authenticity of the clients' identity, his account property, and make sure that he/she is not subject to piracy, the obligations of the service provider is to ensure a software that is difficult to hack.

✓ Material Security: of the network, the applications and the servers, with no security breach therein.

✓ Applications Security: by providing the data processing and programming effective tools.

✓ Privacy and Data Protection: To master self-protection and self-regulation and to ensure that the consumers are aware of the real value of their personal data and know how to raise legal proceedings.

✓ The user must be careful to store the important, sovereign and confidential information on local, not international data storage units.

Awareness Raising and Capacity Building Suggestions

- The importance of issuing a guide on the basics of the cloud computing, determining how to take advantage thereof, and what data may be stored on the cloud and, most importantly, how to make sure that the cloud computing server is internationally recognized.
- To set up the appropriate national authority of cloud computing in every Arab country with communication centers to be established among them.
- To build Arab national skilled capacities, train the law enforcement entities, advance the skills to keep up pace with the social and technological developments in cloud computing, and update the business models to deal with cloud computing matters and the services they provide, those being multinationals alien from the State institutions and departments.
- The importance of promoting ethical and behavioral rules.

- The importance of specialized researches in the legislative framework of the cloud computing, seminars, workshops and trainings.
- The importance for the educational institutions, particularly those of higher education, to recognize the research encouragement mechanisms and to keep up with the developments of cloud computing, smart systems, software, telecommunication and network engineering, data management, processing and transfer and information systems.

II- <u>Regionally</u>

Since the cloud computing technologies are constantly evolving with the massive cross-border data storage, which requires the Arab States keep pace with the changes that arise and consolidate efforts to take the following measures:

- An Arab Safe Harbor Agreement (the suggested terms of which are indicated above).
- The importance of cooperation between Arab States at the regional level and coordinate with the international bodies.
- To set models of "contracts between clients and service providers" free of deception.
- The participation of all concerned stakeholders in establishing an Arab regulatory and legislative structure of cloud computing such as the policymakers in the States, the specialized active regional and international organizations, the coordination bodies, the individual experts and the research institutions, and the representatives of the international companies.
- To put in place guidelines contain harmonized frameworks for the Arab region.
- To exchange Arab and western expertise.

Finally, we quote ITU:

"Indeed, Cybersecurity is a process, not a destination. No country starts from zero, and no country has completed the process".

Commented [AAR1]: The references and the footnotes are missing

BIBLIOGRAPHY

BOOKS:

1. AWAN (Imran), BLAKEMORE (Brian): Policing Cyber Hate, Cyber Threats and Cyber Terrorism – ASHGATE – 2012 – UK .
2. BENSOUSSAN (Alain): Informatics, Télécoms, Internet: Réglementation, contrats, fiscalité, assurance, santé, fraude, communications électroniques – 5e édition – 2012 – Editions Francis LEFEBEVRE.
3. CAPRIOLI (Eric): La sécurité des services de confiance in: Signature électronique et dématérialisation - 2014 – LexisNexis.
4. CHERMAK (Steven), FREILICH (Joshua): Transnational terrorism – ASHGATE – 2013
5. DEBRAS (Jérôme): Guide juridique des contrats en informatiques – Editions ENI – 2013 – France – 38 et suiv.
6. DE MAISON ROUGE (Olivier): Le droit de l'intelligence économique – Patrimoine informationnel et secrets d'affaires – Lamy – 2012 - France P: 85
7. DEMOULIN (Marie), SOYEZ (Sébastien): L'archivage électronique dans le secteur public: entre archivage légal et archivage patrimonial – in: L'archivage électronique et le droit (sous la direction: Marie DEMOULIN) – CRIDS – Larcier – 2012 – Bruxelles – P: 37 et suiv.
8. DEMOULIN (Marie): Les cas spécifique des archives publiques : entre archivage légal et archivage patrimonial – in: L'archivage électronique et le droit – CRIDS – Larcier – 2012 – Bruxelles – P: 91 et suiv.
9. FERAL-SCHUL (Christiane): Cyberdroit, Le droit à l'épreuve de l'internet – 2009-2010 - Dalloz - P:83
10. FITZGERALD (Brian): Cyber-Law – Volume I – The international library of essays in law & Legal theory – Second series – ASHGATE DARTMOUTH – Australia - P: XVII
11. GOLA (Romain): Bases de données et logiciels nécessaires au fonctionnement du site web – in: Droit du commerce électronique – Guide pratique du e-commerce - Gualino - Lextenso Editions – 2013.
12. LE METAYER (Daniel): Les technologies de l'information au service des droits: opportunités, défis, limites – 2010 – Cahiers du Centre d Recherches Informatique et Droit - Bruylant - P: 47
13. LESSIG (Lawrence): The law of the horse: What cyberlaw might teach? – in: CyberLaw – op.cit. - P: 250
14. MATTATIA (Fabrice): Cloud computing - Traitement des données personnelles - Le guide juridique – La loi Informatique et libertés et la CNIL – Jurisprudences – Editions EUROLLES – 2013
15. NELKEN (David): Comparative criminal Justice and Globalization – 2011 – ASHGATE.
16. QUEMENER (Myriam), PINTE (Jean-Paul): L'économie à l'ère numérique – in: Cyber-sécurité des acteurs économiques – risques, réponses stratégiques et juridiques – 2013 - Lavoisier – Paris
17. ROOQUES-BONNET (Marie-Charlotte): Les bases de données de l'Etat: Les fichiers publics – in: Le droit peut-il ignorer la révolution numérique? – Michalon – 2010 – France

Book in Arabic:

EL-KHOURY (Janane): Internationals Economics Crimes & Cross Border Organized Crimes – Sader Ed. – 2009 - Beirut

UNITED NATIONS:

United Nations - General Assembly: Guidelines for the regulation of computerized personal data files – A/RES/45/95 – December 14, 1990.

EUROPEAN UNION:

- US-EU: International Safe Harbor Privacy Principles
- https://en.wikipedia.org/wiki/Safe_Harbor_Principles#cite_note-inval-9
- European Court of Justice 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.) 25 August 2000, retrieved 30 October 2015
- Commission Européenne: Décision 2004/535/EC – JOUE – 235 – 6 JUILLET 2004 –p: 11-22
- http://eur-lex.europa.eu/LexUriSerc/site/en/oj/2004/l_235l_23520040706enoo110022.pdf
- Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security - Official Journal L 0215 , 11/08/2012 P. 5 - 0014
- Jump up to: [abc]"Judgment in Case C-362/14 Maximillian Schrems v Data Protection Commissioner: The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid"(press release) (Press release). Court of Justice of the European Union. 6 October 2015. p. 3. Retrieved 7 October 2015.
- European Parliament and the Council of Europe: Directive 2206/24/EC – on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communications networks and amending Directive 2002/58/EC.
- 2010/87/: Décision de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil [notifiée sous le numéro C(2010) 593] (Texte présentant de l'intérêt pour l'EEE) - OJ L 39, 12.2.2010, p. 5–18
- Directive 2002/19/EC of the European Parliament and of the Council of 7 march2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive
- Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters - OJ L 350, 30.12.2008
- EU Commission: Industry calls for true digital single market in recommendations on European cloud strategy.
- Code of Practice: Protection of personal Data – 2009
- https://dataprotection.ie/documents/code%20of%20practice/RevenueCOP.pdf
- Personal data protection: processing and free movement of data (General Data Protection Regulation)
- http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2012/0011%28COD%29
- Cloud computing: A legal maze for Europe / Euractiv, 18/4/2012 - Overview of cloud computing, its benefits and the associated legal issues.http://www.euractiv.com/innovation-enterprise/cloud-computing-legal-maze-europe-linksdossier-511262
- OECD: Guidelines on the protection of privacy and Transborder flow of Personal data – 1980 – www.oecd.org/document/18/0,23,40en_2649_34255_1815186_1_1_1_1,00.html
- Council of Europe: Convention on the protection of individuals with regard to automatic processing of personal data – 1980

Local Legislations:

1. Canada: Personal Information Protection and Electronic Documents Act, 2000
2. Patriot Act – 2001 – USA
3. **FRANCE**:
   - Code de la santé publique, dernière modification: 1 juillet 2014

- Décret No. 960/2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique et modifiant le code de la santé publique (dispositions réglementaires) – 15 mai 2007.
- Loi N°.78/17 du 6 janv. 1978 – relative à l'informatique, aux fichiers et aux libertés – J.O. – 7 janv. 1978 – www.legifrance.gouv.fr
- Loi N°.88/227 – du 11 mars 1988 – Loi relative à la transparence financière de la vie politique – J.O. – 12 mars 1988;
- Loi N°92–1336 - 16 décembre 1992 - relative à l'entrée en vigueur de nouveau code pénal – J.O. – 23 déc. 1992 – www.legifrance.gouv.fr;
- Loi N°.94-548 – 1er Juillet 1994 - relative au traitement des données nominatives ayant Pour fin la recherche dans le domaine de la santé - J.O. - 2 juillet 1994;
- Loi N°. 2000/321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations – J.O. – No. 88 – 13 avril 2000 – P: 5646;
- Loi N°.2003/239 du 18 mars 2003 pour la sécurité intérieure – J.O. – 19 mars 2003; Loi N°.57/298 du 11 mars 1957 sur la propriété littéraire et artistique – www.legifrance.gouv.fr
- Loi N°.2004/801 – du 6 août 2004 – relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel – et modifiant la loi No. 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés - J.O. – N°. 182 – 7 août 2004 – P: 14063
- Loi 801/2004 – pour la confiance dans l'économie numérique – 21 juin 2004

Arabic LAWS:

Jordan:

- The telecommunications law n°13/1995, which was rectified by amendment law n°21/2011 (official gazette n°4072 of October 1st, 1995).
- The temporary law on public statistics - 2008
- Information System Crimes Law n°(30) of 2010 was promulgated (official gazette n°5056 dated September 16, 2010 - page 5334)

United Arab Emirates (UAE):

- The UAE penal code (n°3/1987)
- The "Emirates Telecommunications Corporation" act (n°1/1991),
- Act n°3/2003 on regulation of the telecommunications sector.
- Act n°2 on e-transactions and e-commerce – 2002
- The federal law n°1/2006 on e-transactions and e-commerce – January 3, 2006;
- the Federal Law n°2/2006 on Combating Cybercrimes,
- Law on Personal Data protection – no. 11/2006 – UAE - 2006
- Decree-Law n°5/2012 on Combating Cybercrimes, August 13, 2012; Abu Dhabi as a replacement for Law n°2 of 2006;
- the Dubai Law on data publication and exchange (open data law of October 17, 2015);
- The special law of the Dubai International Financial Center DIFC, No 1/2007 on the protection of its own data and lists

- The circular n°6 on the Abu Dhabi government's data security policy and standards – 2013;
- Departmental order n°21/2013 on Information Technology (IT) - 2013
- Dubai law 2002 with relation to the establishment and protection of telecommunications network.
- Departmental order n°13 on the data security in Dubai Emirate - The executive council - January 27, 2012.

BAHRAIN:

- The telecommunications and Internet law n°48/2002
- Law n°28/2002 on e-transactions and e-commerce
- Law n°60/2014 on IT crimes
- The decree n°9/2002 on reorganization of the Central Informatics Organization (CIO)
- The Decree n°25/2005 on the establishment of the High Committee on ICT

Algeria

- law n°09-04 of 14 Shaaban 1430 H (August 5, 2009) to regulate the prevention and fighting of IT-and communication-related crimes.

Kingdom of Saudi Arabia (KSA)

- Anti-Cybercrime Law issued in 2007 (Royal Decree n°M/17 dated 8/3/1428 H)
- Departmental order n°40 of March 27, 2006 on the regulations governing the public e-transactions, Council of Ministers - KSA
- Departmental order n°6667 of 1/7/1426 H, on the conditions of practice of consulting in the ICT sector - Council of Ministers - KSA.

Sudan

- The e-transactions law 2007- Sudan
- The counter-cybercrime law – 2007 - Sudan

Iraq:

- The trademarks and commercial data law n°21/1975, amended by law of January 4, 2010 - Iraq
- The consumer protection law n°1 of January 4, 2010 - Iraq
- The law n°78 on the electronic signature and e-transactions - 2012 - Iraq.

Kuwait:

- The law by decree n°5/1999 concerning Intellectual Property Rights – 1999 – Kuwait
- The Communication and Information Technology Regulatory Authority (CITRA) – 2014 - Kuwait

Morocco:
- The law n°08-09 on the protection of people from the processing of personal data – February 23, 2009
- The law n°07-03 as complementary to the laws constituting the criminal code related to crimes of breach of electronic data processing system – 2003
- The law n°05.53 on the digital exchange of electronic data
- The law n°31-08 which sets measures for consumer protection - 2008

Yemen:
- The law n°40/2006 on the regulations of payment, electronic financial and banking transactions - 2006.
- Presidential decree n°155/1995, established the National Information Center
- The departmental order of the Council of Ministers n°4/2002, to create the Communication and Information Technology City

Tunisia
- The law n°38/1998 on the post magazine,
- The law n°19/1998 on rectification and completion of some provisions of the criminal law was passed as a way to protect data, digital services and software.
- The law n°83/2000 on electronic exchange and commerce,
- The telecommunication law n°1/2001
- law n°63/2004 on personal data protection –
- law n°5/2004 on regulation of the information security and control of the general rules to protect the computer systems and the networks,
- Laws n°1249/2004 and n°1250/2004)
- Directive n°31 of 2007 on the establishment of the digital economy

Djibouti:
- The law n°28/2008 on protection, suppression of fraud and consumer protection,

Sultanate of Oman:
- The e-transactions law n°69/2008
- the IT crime fighting law promulgated by royal decree n°12/2011 (official gazette n°929 dated February 6, 2011),

Syria

- The law n°4/2009 adopted the digital signature and network services - 2009
- The telecommunications law n°18/2010
- The Media law was issued by Legislative-Decree n°108 of August 8, 2011.
- The decree-law n°17/2012 to regulate communications over the Internet and combat cybercrime.

Palestine:

- The 2009 e-transactions law.
- Law on protection of personal data and information - on April 12, 2016.
- The departmental order n°20/2001 created the Palestinian National Internet Naming Authority.
- The Palestinian Cabinet departmental order n°35/2004 on the right to access the Internet and the e-mail through the Government Computer Center.
- The Cabinet departmental order n°3/2004 on the prevention of sale and of marketing of communications services, information technology and express mail.
- The Cabinet departmental order n°26/2005 on the approval of public policies to use the computer and the Internet in the public institutions.
- The Cabinet departmental order n°74/2005 on the national strategy of the information technology and.
- The Cabinet departmental order n°65/2005 on the approval of the adoption of the E-Palestine initiative.
- Decision n°11/41/14/C.M./C.S. of February 19, 2013 on the adoption of the Palestinian Interoperability Framework "Zinnar".
- Decision n°08/127/13/C.M./C.S. on the adoption of the information security policy document.
- Decision n°08/46/14/C.M./C.S. of March 12, 2013 on the formation of a Palestinian computer emergency response team (information security).
- Decision n°08/45/17/C.M./R.H. on the formation of the e-government permanent central team.
- Decision n°22/24/16/C.M./R.H. on the formation of the supreme ministerial committee.

Qatar:

- The anti-cybercrime law n°14 of 2014,
- The Qatari telecommunications law n°34/2006

- The law of the Qatar Financial Centre (QFC), No. 7/2005 -
- The e-transactions and e-commerce law n°16/2010 (August 19, 2010)

Lebanon:

- The law n°140 of October 27, 1999 on protection of the right to confidential phone conversations.

Egypt:

- The law n°10 of 2003 on regulation of communications – 2003 – Egypt
- The law n°120 of 2008 – 2008 - Egypt

[1] Le Cloud Computing: un défi pour la loi informatique et libertés? – http://www.zdnet.fr/actualites/saas-et-legislation-europeenne-ce-qu-il-faut-savoir-39794305.htm
[2] MATTATIA (Fabrice): Cloud computing - Traitement des données personnelles - Le guide juridique – La loi Informatique et libertés et la CNIL – Jurisprudences – Editions EUROLLES – 2013 – P: 19
[3] CISCO: http://www.datacenterknowledge.com/archives/2012/10/23/cisco-releases-2nd-annual-global-cloud-index/
[4] LESSIG (Lawrence): The law of the horse: What cyber law might teach? – in: Cyber Law – Volume I – The international library of essays in law & Legal theory – Second series – ASHGATE DARTMOUTH – Australia . - P: 250.
[5] LE METAYER (Daniel): Les technologies de l'information au service des droits: opportunités, défis, limites – 2010 – Cahiers du Centre de Recherches Informatique et Droit - Bruylant - P: 47
[6] FITZGERALD (Brian): Cyber-Law – Volume I – The international library of essays in law & Legal theory – Second series – ASHGATE DARTMOUTH – Australia - P: XVII
[7] GOLA (Romain): Bases de données et logiciels nécessaires au fonctionnement du site web – in: Droit du commerce électronique – Guide pratique du e-commerce - Gualino - Lextenso Editions – 2013 - P: 181 et suiv.

[8] BENSOUSSAN (Alain): Informatics, Télécoms, Internet: Réglementation, contrats, fiscalité, assurance, santé, fraude, communications électroniques – 5e édition – 2012 – Editions Francis LEFEBEVRE - Définition du cloud computing - P: 352
[9] ITU - No. 1 – 2013 -https://itunews.itu.int/ar/Note.aspx?Note=3727
[10] Deloitte Gov2020 – A journey into the future of Government - www2.deloitte.com public.sector
[11] ITU - ibid - https://itunews.itu.int/ar/Note.aspx?Note=3727
[12] BENBOUSSAN:Traitement fiscal - Chapitre I: Logiciels – in: op.cit. - P: 690 et suiv
[13] CAPRIOLI (Eric): La sécurité des services de confiance in: Signature électronique et dématérialisation - 2014 - LexisNexis – P: 248

[14] Soecial Eurobarometer 359 – Report june 2011 – Attitudes on Data Protection and Economic Idendity in the European Union
https://itunews.itu.int/Ar/Note.aspx?Note=3726
[15]Study presented to ESCWA – August 2015

[16]
http://www.moict.gov.jo/documents/%D9%88%D8%AB%D9%8A%D9%82%D8%A9%20%D8%A7%D9%84%D8%B3%D9%8A%D8%A7%D8%B3%D8%A9%20%D8%A7%D9%84%D8%B9%D8%A7%D9%85%D8%A9%20%D9%84%D9%84%D8%AD%D9%83%D9%88%D9%85%D8%A9%202003.pdf

[17] Dubai act n°2 on e-transactions and e-commerce - February 12, 2002 - Dubai
http://www.sca.gov.ae/arabic/legalaffairs/LegalLaws/Electronic_Trading_Transaction.pdf
[18] Federal law n°1/2006 on e-transactions and e-commerce – January 3, 2006 – Abu Dhabi
http://www.dubaided.ae/Arabic/DataCenter/BusinessRegulations/pages/federallaw1of2006.aspx
[19] The Federal Law n°2/2006 on Combating Cybercrimes the Federal Law n°2/2006 on Combating Cybercrimes - UAE
http://www.f-law.net/law/threads/ -
[20] passed Federal Decree-Law n°5/2012 on Combating Cybercrimes – August 13, 2012 – Abu Dhabi
http://www.wipo.int/wipolex/ar/details.jsp?id=13909
[21] ESCWA: Policy Recommendations on Cybersafety and Combating Cybercrime in the Arab Region - E/ESCWA/TDD/2015/1 – 2016 https://www.unescwa.org/publications/policy-recommendations-cybersafety-arab-region

[22] www.aecert.ae

[23] The special law of the Dubai International Financial Center (DIFC)on the protection of its own data – no. 1 – 2007 -
http://dp.difc.ae/legislation/dp_protection/
[24] European Parliament and Council Directive – 95/46/EC of 24 October 1995 – on the protection of individuals with regard to the processing of personal data and on the free movement of such data – Official Journal – L 281 – 23.11. 1995
[24]http://www.emaratalyoum.com/local-section/other/2015-10-17-1.831307
[25] http://www.emaratalyoum.com/local-section/other/2015-10-17-1.831307
[26] http://bibliotdroit.blogspot.com/2016/03/blog-post_185.html
[27] http://www.wam.ae/ar/news/emirates/1395239228828.html
[28] http://www.mcit.gov.sa/Ar/InformationTechnology/Pages/IntentionalNews/Tech-News-Inte-21081435_590.aspx
[29] www.cert.gov.sa
[30] http://www.cert.sd/ar/index7bd7.html
[31] Sudan e-Governement - http://www.sudan.sd/policy.aspx
[32] http://www.moj.gov.iq/uploaded/4274.pdf
[33] https://www.cait.gov.kw/National-Projects/Kuwait-Information-Network.aspx
[34] https://www.cait.gov.kw/
[35] http://www.gcc-legal.org/LawAsPDF.aspx?country=1&LawID=4100
[36] The law n°08-09 on the protection of people from the processing of personal data – February 18, 2009 - official gazette n°5711 dated February 23, 2009 - Morocco

[37] http://www.justice-lawhome.com/vb/archive/index.php?t-9166.html
[38] www.tuncert.ansi.tn
[39] http://www.anrtic.km/
[40] An opportunity to boost access to basic services in health and education - WIMAX – 19 december 2013
https://itunews.itu.int/En/4954-An-opportunity-to-boost-access-to-basic-services-in-health-and-education.note.aspx
[41] I have revised it personally in august 2015
[42] www.cert.gov.om
[43] www.nans.gov.sy
[44] www.sytra.gov.sy
[45] The strategy of the e-government in Syria http://www.moct.gov.sy/moct/?q=ar/node/61
[46] the "National Information Security Policy" in Syria
http://nans.gov.sy/images/stories/doc/isc_doc/finalpolicy.pdf
[47] http:// www.moct.gov.sy/ICTSandards/ar_pdf/2.pdf
[48] the anti-cybercrime law n°14 of 2014 –
http://www.almeezan.qa/LawPage.aspx?id=6366&language=ar
http://www.almeezan.qa/mojportal/LawView.aspx?opt&LawID=3987&language=ar[49]انون
[50] Qatar Financial Center (QFC) special rules on the protection of its own data and lists
http://www.complinet.com/net_file_store/new_rulebooks/q/f/QFCRA_1559_VER1_ARABIC.doc
[51] www.qcert.org
[52] The Lebanese Republic - Tthe Lebanese Ministry of Telecommunications - the Vision of Digital Communications for 2020 – July 1, 2015 -
http://www.mpt.gov.lb/index.php/ar/2013-02-17-13-15-34/mpt-news-ar/50-latest/373-2015-07-01-15-17-30
[52]http://cim.gov.ly/page95.html
[53] ttp://cim.gov.ly/page95.html
[54] I Have revised it personally
[55] http://www.mcit.gov.eg/Ar/TeleCommunications/Telecom_Act_Law/Telecom_Act
[56] http://www.egcert.eg/
[57] http://www.ntra.gov.eg/arabic/main.asp
[58] https://itunews.itu.int/ar/Note.aspx?Note=3728
[59] http://www.alecso.org/cloud/

[60] Principle of lawfulness and fairness, Principle of accuracy, Principle of the purpose-specification, Principle of interested-person access, Principle of non-discrimination, Power to make exceptions, Principle of security, Supervision and sanctions, Transborder data flows

[61] United Nations - General Assembly: Guidelines for the regulation of computerized personal data files – A/RES/45/95 – December 14, 1990.

[62]BASIC PRINCIPLES OF NATIONAL APPLICATION: Collection Limitation Principle, Data Quality Principle, Purpose Specification Principle, Use Limitation Principle, Security Safeguards Principle, Openness Principle, Individual Participation Principle, Accountability Principle -

.Annex to the Recommendation of the Council of 23rd September 1980: GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA – https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[63] ESCWA - reports on Cyber Legislation – 2012 - https://www.unescwa.org/cyber-legislation http://isper.escwa.un.org/Portals/0/Cyber%20Legislation/Regional%20Harmonisation%20Project/Directives/Dir-4-DataProtection.pdf

[64] BENBOUSSAN: Traitement des opérateurs acheminant du trafic international – in op.cit. – P: 798
[65] FERAL-SCHUL (Christiane): Cyberdroit, Le droit à l'épreuve de l'internet – 2009-2010 - Dalloz - P:83
[66] US-EU: International Safe Harbor Privacy Principles https://en.wikipedia.org/wiki/Safe_Harbor_Principles#cite_note-inval-9
[67] European Court of Justice 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.) 25 August 2000, retrieved 30 October 2015.
[68] Commission Européenne: Décision 2004/535/EC – JOUE – 235 – 6 JUILLET 2004 –p: 11-22 http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_235l_23520040706enoo110022.pdf
[69] Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security - Official Journal L 0215 , 11/08/2012 P. 5 - 0014

[70] Jump up to: [abc]"Judgment in Case C-362/14 Maximillian Schrems v Data Protection Commissioner: The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid"*(press release) (Press release). Court of Justice of the European Union. 6 October 2015. p. 3.Retrieved 7 October 2015.*
[71] European Parliament and the Council of Europe: Directive 2006/24/EC – on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communications networks and amending Directive 2002/58/EC.
[72] 2010/87/: Décision de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil [notifiée sous le numéro C(2010) 593] (Texte présentant de l'intérêt pour l'EEE) - OJ L 39, 12.2.2010, p. 5–18
[73] Directive 2002/19/EC of the European Parliament and of the Council of 7 march2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive).

[74] Convention on Cybercrime (Budapest, 23 November 2001), http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[75] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters OJ L 350, 30.12.2008
[76] EU Commission: Industry calls for true digital single market in recommendations on European cloud strategy.
[77] Code of Practice: Protection of personal Data – 2009
https://dataprotection.ie/documents/code%20of%20practice/RevenueCOP.pdf
[78] Personal data protection: processing and free movement of data (General Data Protection Regulation)
http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2012/0011%28COD%29
[79] **Cloud computing: A legal maze for Europe** / Euractiv, 18/4/2012 - Overview of cloud computing, its benefits and the associated legal issues.http://www.euractiv.com/innovation-enterprise/cloud-computing-legal-maze-europe-linksdossier-511262
[80] DEMOULIN (Marie), SOYEZ (Sébastien): L'archivage électronique dans le secteur public: entre archivage légal et archivage patrimonial – in: L'archivage électronique et le droit (sous la direction: Marie DEMOULIN) – CRIDS – Larcier – 2012 – Bruxelles – P: 37 et suiv.
[81] Canada: Personal Information Protection and Electronic Documents Act, 2000
[82] UK: Data Protection Act – 1998 – www.legislation.gov.uk
[83] USA Patriot Act – October 2001 - www.justive.gov.usa
[84] Commission nationale de l'informatique et des libertés CNIL: Guide sur les transferts de données à caractère personnel vers des pays non membres de l'union européenne. – 2008 - http://www.cnil.fr/fileadmin/images/la_cnil/actualite/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf
[85] BENBOUSSAN: Traitements automatisés – Champs d'application de la loi – in: op.cit. - P: 508
[86] Mattatia Transfert de données hors de l'Union européenne – En Pratique: devant les tribunaux et la CNIL – in: op.cit. - P: 156
[87] Loi N°.78/17 du 6 janv. 1978 – relative à l'informatique, aux fichiers et aux libertés – J.O. – 7 janv. 1978 – www.legifrance.gouv.fr
[88] Loi N°.88/227 – du 11 mars 1988 – Loi relative à la transparence financière de la vie politique – J.O. – 12 mars 1988; Loi N°92–1336 - 16 décembre 1992 - relative à l'entrée en vigueur de nouveau code pénal – J.O. – 23 déc. 19 92 – www.legifrance.gouv.fr; Loi N°.94-548 – 1er Juillet 1994 - relative au traitement des données nominatives ayant Pour fin la recherche dans le domaine de la santé - J.O. - 2 juillet 1994; Loi N°. 2000/321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations – J.O. – No. 88 – 13 avril 2000 – P: 5646; Loi N°.2003/239 du 18 mars 2003 pour la sécurité intérieure – J.O. – 19 mars 2003; Loi N°.57/298 du 11 mars 1957 sur la propriété littéraire et artistique – www.legifrance.gouv.fr
[89] Loi N°.2004/801 – du 6 août 2004 – relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel – et modifiant la loi No. 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés - J.O. – N°. 182 – 7 août 2004 – P: 14063
[90] Convention for the protection of individuals with regard to Automatic Processing of Personal Data - 24.1.1981 – http://convenyions.coe.int/Treaty/FR/Treaties/Html/108.htm.
[91] Loi 801/2004 – pour la confiance dans l'économie numérique – 21 juin 2004
[92] Cass. Civ.: 1ere Chambre civile – 9 décembre 2003.
[93] Jurisprudences pour le statut de données personnelles: Conseil d'Etat – 10e et 9e sous-sections réunies – No. 288149 – 23 mai 2007; TGI Bobigny: 15e chambre – 14 décembre 2006; C.A Rennes: 3e chambre - 22 mai 2008; CA Rennes: 3e Chambre 23 juin 2008
[94] Jurisprudences contre le statut de données personnelles: C.A. Paris: 13e chambre – section B – 27 avril 2007; C.A. Paris: 13e chambre section A – 15 mai 2007.
[95] LOI n°2015-912 du 24 juillet 2015 - art. 4
https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006418316&cidTexte=LEGITEXT000006070719
[96]. Article 323-1: Fraudulent accessing or remaining within all or part of an automated data processing system is punished by a sentence not exceeding two years' imprisonment and a fine of 30.000 euro.

Where this behaviour causes the suppression or modification of data contained in that system, or any alteration of the functioning of that system, the sentence is not exceeding three years' imprisonment and a fine of 45.000 euro.

Article 323-2: Obstruction or interference with the functioning of an automated data processing system is punished by a sentence not exceeding five years' imprisonment and a fine of 75.000 euro.

Article 323-3: The fraudulent introduction of data into an automated data processing system or the fraudulent suppression or modification of the data that it contains is punished by a sentence not exceeding five years imprisonment and a fine of 75.000 euro.

[97] Décret No. 2008-632 – 27 juin 2008 – Portant création d'un traitement automatisé de données à caractère personnel dénommé "EDVIGE" – J.O. – 1 juillet 2008 – No. 0152

[98] UN: Guidelines for the regulation of computerized personal data files - The General Assembly - A/RES/45/95 - 68th plenary meeting- 14 December 1990;

Council of Europe: Convention on the protection of individuals with regard to automatic processing of personal data – 1980

OECD: Guidelines on the protection of privacy and Transborder flow of Personal data – 1980 – www.oecd.org/document/18/0,23,40en_2649_34255_1815186_1_1_1_1,00.html

[99] BENBOUSSAN: informatique et atteintes aux intérêts fondamentaux de la nation: Trahison et espionnage – in: op.cit. – P: 921

[100] JHOSON (David): Law and Borders: The rise of law in cyberspace – in cyberlaw – op.cit. – P: 419

[101] MICONNET (Thomas): Le Cloud computing - un nuage d'insécurités juridiques – 2013 http://avocats-publishing.com/Le-Cloud-computing

[102] BENSOUSSAN: Caractéristiques du recours aux services de type cloud computing - op.cit. P: 371

[103] **ITU** -https://itunews.itu.int/ar/Note.aspx?Note=3727

[104] El-(KHOURY) Janane: Internationals Economics Crimes and the cross border organized crimes – 2009 – Sader - Beirut – P: 415

[105] NELKEN (David): Comparative criminal Justice and Globalization – 2011 – ASHGATE – P: 69

[106] Especially all kinds of cross-border illegal traffic, ex.: Traffic of drogues, traffic of weapons, human traffic, traffic of human organs, money laundering, terrorism financing….

[107] CHERMAK (Steven), FREILICH (Joshua): Transnational terrorism – Ashgate – 2013 – P: 3

[108] AWAN (Imran), BLAKEMORE (Brian): Policing Cyber Hate, Cyber Threats and Cyber Terrorism – ASHGATE – 2012 – UK - P: 149

[109] DEMOULIN (Marie): Les cas spécifique des archives publiques : entre archivage légal et archivage patrimonial – in: L'archivage électronique et le droit – CRIDS – Larcier – 2012 – Bruxelles – P: 91 et suiv.

[110] ROOQUES-BONNET (Marie-Charlotte): Les bases de données de l'Etat: Les fichiers publics – in: Le droit peut-il ignorer la révolution numérique? – Michalon – 2010 – France - P: 23

[111] Gola: Droit du commerce électronique – guide pratique du e-commerce – op.cit. – 402 et suiv.

[112] DEBRAS (Jérôme): Guide juridique des contrats en informatiques – Editions ENI – 2013 – France–38.

[113] https://itunews.itu.int/Ar/Note.aspx?Note=3726

[114] QUEMENER (Myriam), PINTE (Jean-Paul): L'économie à l'ère numérique – in: Cyber-sécurité des acteurs économiques – risques, réponses stratégiques et juridiques – 2013 - Lavoisier – Paris - P: 165

[115] BENSOUSSAN (Alain): Exploitations des bases de données privées – in: Informatiques, Télécoms, Internet – 5e édition – Editions Francis LEFEBVRE – 2013 - P: 245 et suiv.

[116] DE MAISON ROUGE (Olivier): Le droit de l'intelligence économique – Patrimoine informationnel et secrets d'affaires – Lamy – 2012 - France P: 85