Cloud Computing in Arab States: Legal Aspect, Facts and Horizons

ITU-ATU Workshop on Cybersecurity Strategy in African Countries

Khartoum, Sudan, 24-26 July 2016

Rouda AlAmir Ali
Programme Officer
ITU Arab Regional Office

Overview

- The concept of Cloud Computing
- Practical Challenges and Legal Issues Raised in Arab Countries
- Legislative and Regulatory Situation Exclusively in 22 Arab Countries
- Best Practices of the Cloud Computing Legal Framework: Comparative Study United Nations, ITU and Cloud Computing
- The European Union's Leading Role
- Western Local Legislations
- Legal Standards, Regulations and Legal Suggestions
- Contractual Aspect of the Cloud Computing Legal Framework: Suggestions and Standards
- National Sovereignty, Cloud Computing Security and Cross-border Security Challenges
- Regional Coordination and Cooperation between Arab Countries
- Arab Safe Harbor Agreement
- Conclusion and Proposals

Abstract

- The study aims at reviewing the legal and legislative aspects of cloud computing in the Arab States: facts and horizons.
- Tackles the 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.

Introduction:

- Cloud computing is considered as one of the greatest technological transformations and breakthroughs in the world.

- It offers 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.

- Cloud computing creates lots of challenges in the Arab countries, mostly at the legal, executive, administrative, technical and practical levels.

Practical Challenges and Legal Issues Raised in Arab Countries

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

- The ability to get the latest developed applications and software at reasonable prices;
- The loss of tax revenues due to the absence of the tax administration with respect to any sale, assignment or purchase of a database;
- 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, 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;
- The slow and/or costly Internet connection in some countries;
- The lack of a digital infrastructure in the Arab countries;
- The insufficiency of information security in cloud computing;
- The lack of information security in relation to some of the governmental institutions;
- 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.

Legal and Regulatory Situation in Arab States:

- The legal issue of the cloud computing brings up lots of problems particularly in the Arab States where no particular laws were enacted to protect the databases and the data in general.
- Few Arab States have adopted special law dedicated to personal data protection. There are only fragmented texts introduced in separate legislations.
- Most of the Arab countries have no mechanisms to apply the elaborated rules.
- The local and sovereign traditional principles now face some challenges.
- Many of the laws in the Arab States h**ave been amended**, particularly the criminal law and the civil law, in order to include the legal protection of information, data, intellectual property and digital documents, etc.
- Many laws **have been enacted with respect to the information technology, the electronic transactions, the e-commerce and the cybercrimes**.
- The **Gulf Countries** are among the first Arab countries that have paved the way for the cloud computing.

1. Algeria:

- Law n°09-04 of 14 Shaaban 1430 H (August 5, 2009) regulates prevention and fighting of IT-and communication-related crimes.
- Draft-law related to the “electronic authentication and signature”.

2. Bahrain:

- Law n°48/2002 incriminates any alteration, interception or disclosure of communications and of their content (article 75 thereof);
- Law n°28/2002 on e-transactions and e-commerce;
- Law n°60/2014 on IT crimes and Data protection;
- 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.

3. Comoros:

Legislative lack.

4. Djibouti:

- Law n°28/2008 on protection, suppression of fraud and consumer protection.

5. **Egypt**:

- Law n°10 of 2003 on regulation of communications;
- The Egyptian Computer Emergency Response Team, EG-CERT (2010);
- The National Telecommunication Regulatory Authority (NTRA).

6. **Iraq**:

- The trademarks and commercial data law n°21/1975, amended by law of January 4, 2010, including consumer protection;
- Law n°78/2012 on the electronic signature and e-transactions;
- The national strategy and the plan of action of the Iraqi e-government 2012-2015.

7. Jordan:

- Temporary law of 2008 on public statistics;
- Law n°30 of 2010 on software crimes;
- The communications and telecommunications law n°13 of 1995, amended by law n°21 of 2011;
- The National Information Technology Center;
- The "National Center for Security and Crisis Management“.

8. Kingdom of Saudi Arabia (KSA):

- Cloud computing has been widely adopted in business and international investments in KSA;
- The Kingdom's anti-cybercrime regulation;
- Executive Decision n°40 of March 27, 2006 on the regulations governing the public e-transactions; and departmental order n°6667 of 1/7/1426 .

9. Kuwait:

- Law n°5 of 1999 on the protection of copyright for material published in all media and Law n°37/2014; and a draft law on the e-transactions;
- National initiatives to revitalize the electronic archive and cloud computing applications;
- Major role for the Central Agency for Information Technology (CAIT);
- The Communication and Information Technology Regulatory Authority (CITRA) (by law n°37/2014).

10. Lebanon:

- Law n°140 /1999 on protection of the right to confidential phone conversations;
- Draft law, ECOMLEB on Personal Data;
- Participation with the ITU in the Study Group 17 meetings of the Telecommunication Standardization Sector;
- The role of the Telecommunications Regulatory Authority (TRA);
- In 2015, launching of the Vision of Digital Communications for 2020;
- Suffering from the lack of specialized legislations and of procedural regulations.

11. Libya:

- Suffering from the lack of specialized legislations and of procedural regulations;
- in 2015, launching LCNA, the first Libyan cloud computing-based news agency.

12. Mauritania:

- In 2015, launching a new generation of storage and cloud computing solutions in Gitex;
- Suffering from the lack of specialized legislations and of procedural regulations.

13. Morocco:

- The new Moroccan Constitution n°1.11.91 of 27 Shaaban 1432 H;
- Law n°08-2009, on the protection of people from the processing of personal data;
- Law n°07-03 as complementary to the laws constituting the criminal code related to crimes of breach of electronic data processing system;
- Law n°05.53 on the digital exchange of electronic data;
- Law n°31-08 for consumer protection.
- The National Control Commission for the Protection of Personal Data (CNDP).

14. Palestine:

- The public statistics law n°4/2000 on the right to access statistical information;
- The departmental order n°20/2001 which created the Palestinian National Internet Naming Authority;
- **Many Executive Decisions**: on accessing the Internet through a Government Computer Centre (N°35/2004), on the validity of contracts executed through electronic mail (N°39/2004), on general policies of the use on the computer and Internet in the official institutions (N°269/2005), on a national strategy for telecommunications and information technology (N°74 /2005), and on the adoption of the E-Palestine Initiative (N°65 of 2005);
- The e-transactions law, in 2010, to regulate the technology industry work.

15. Qatar:

- In 2011, cloud computing was a main controversial topic in Qatar;
- The Qatar Constitution of 2003;
- Telecommunications law N°34 of 2006;
- E-transactions and e-commerce law n°16/2010 (August 19, 2010);
- The role of Qatar Financial Center (QFC);
- Qatar Computer Emergency Response Team (Q-CERT).

16. Somalia:

- Suffering from the lack of specialized legislations and of procedural regulations.

17. Sudan:

- The Sudanese Constitution;
- The e-transactions law and the counter-cybercrime law, in 2007;
- In 2010, Sudan created the Sudan CERT Information Security Center.

18. Sultanate of Oman:

- The e-transactions law n°69/2008 on data protection;
- The IT crime fighting law promulgated by royal decree n°12/2011 (official gazette 929 - dated February 6, 2011) and Law n°13/2009;
- In 2010, the Sultanate of Oman set up Oman's National Computer Emergency Readiness Team, "O-CERT", and hosted the ITU-Regional Cybersecurity Center for the Arab Region.

19. Syria:

- The digital signature and network services law n°4/2009 which created the **National Authority for Network Services;**
- Law n°18/2010 where article 50 establishes the “privacy respect” principle;
- The information law was issued by decree-law n°108/2011 on regulation of the means of communication on the Web;
- The decree-law n°17/2012 on regulation of the communication on the Web and countering of IT crimes;
- The law n°290/2012 for the coordination of the illustrative and executive instructions;
- In 2009-2010, a detailed strategy of the e-government;
- Adopting a series of standards for the ICTs, including protection of ICTs;
- In 2014, the “National Information Security Policy”.

20. Tunisia:

- In 1998, law n°38 on the post magazine, and law n°19 on rectification and completion of some provisions of the criminal gazette was passed as a way to protect data, digital services and software;
- Law n°83/2000 on electronic exchange and commerce;
- Law n°1/2001 to regulate the communications field and provide the basic services of communications and TV and radio broadcasting;
- In 2004, Law n°63 on personal data protection and law n°5 on regulation of the information security and control, and which gave rise to the **National Agency of Information Security (ANSI);**
- Several laws (laws n°1249/2004 and n°1250/2004) were subsequently enacted to put into force law n°5/2004;
- Directive n°31 of 2007 on the establishment of the digital economics;
- In 2007, the ANSI created **tunCERT**.

21 . 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;
- The UAE penal code;
- The “Emirates Telecommunications Corporation” act (1/1991);
- The act n°3/2003 on regulation of the telecommunications sector;
- Law No. 2 of 2002 on e-commerce and e-signature (Dubai);
- The Dubai law n°5/2004 on the information security Federal law N°2 of 2006, on combatting information technology crimes;
- The executive council issued executive decision n°13 on the data security in Dubai Emirate in 2012;
- Federal law on anti-cybercrime N°5 of 2012;
- The circular n°6, in 2013 on the Abu Dubai government’s data security policy and standards;
- Executive Decision N°21 of 2013 on Information Technology (IT) security regulations at federal government entities;
- The Dubai Law on data publication and exchange (open data law of October 17, 2015);
- The Dubai “e-security and anti-cybercrimes center” in 2014;

22. Yemen:

- Law N°40 of 28 December 2006 concerning e-payment, e-banking and financial operations, e-contract and e-signature;
- The presidential decree n°155/1995, established the National Information Center;
- Executive Decision No. 4 of 2002 by the Council of Ministers.

Legal Standards, Regulations and Legal Suggestions

- The major multinational corporations still control the Arab market in the cloud computing field, such as: Microsoft, Amazon, Google, etc.
- 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 , 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.

Legal Standards, Regulations and Legal Suggestions (Cont.)

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; one of which is the preparation of contracts and agreements which ensure service quality and security and data protection. The main concern, being the 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
  - The appropriate mechanisms to deal with the legal and security issues and effects of the services provided by such computing technology.

- 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
  - The users' contracts, including the service request contracts and the paid-for and free-of-charge services contracts;

- The signature of the contract is one of the most important and critical phases due to the main problems 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.

- Therefore, the consumer must make diligent efforts prior to the signing of the contract with the service providers.

There are other issues to be considered such as:

- Data Security:

  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 hand over of the original copies and the destruction of all other backup copies

- Obligation of protection:

  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.

- Management of Big Data;
- Consumer Protection;
- National Sovereignty, Cloud Computing Security and Cross-border Security Challenges:

  Not all the databases require the same level of protection: There are sensitive data concerning the national security and the economic security (bank secrecy).

Regional Coordination and Cooperation between Arab Countries

- There is no constitution in the Arab region that provides 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.
- 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.

Regional Coordination and Cooperation between Arab Countries

Arab Safe Harbor Agreement:

- To set common standards and determine the cross-border information flow requirements;
- To achieve a regulatory process 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 which includes 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 an agreement.

Arab Safe Harbor Agreement(cont.):

- 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 in the case of a 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 the same or the recovery of a 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 the individual state's 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

Conclusion and Proposals:

- The cloud computing creates challenges in Arab States related to contracting, security, data privacy protection, national sovereignty and legislative and regulatory framework.
- 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 levels.
- Most Arab countries have not yet 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.
- 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.
- The Arab States are recommended to set up their own IAAS services in order to keep their data and information safe. The national security-related information must be always under the State sovereignty. Thus, they need a special cloud protected by civil servants and it would create lots of job opportunities for the Arab youth.

Proposals at the local level:

1. Legislative Proposals:

- The importance of reviewing the applicable laws, in order to update or develop the legislative environment for the use of cloud computing services:, the suitable laws and regulations, the executive decrees and the practical decisions.
- The participation of the public policy makers in the States in drawing up local policies.
- To enact laws on new taxes to be levied and to introduce the 4G band to all the regions.

2. Executive Proposals

- To enhance the administrative environment to put laws into force and control the mechanisms;
- The contribution of the State to enable local companies to create an environment of technologies;
- To take advantage of the best practices and successful experiences at the international level, and to adopt the international standards and norms;
- To take into consideration the following issues: Data protection; Identity Management System, Material Security, Applications Security, Privacy and Data Protection.

Awareness Raising and Capacity Building Suggestions:

- The importance of issuing a detailed guide on the basics of the cloud computing;
- To set up the appropriate national authority of cloud computing in every Arab State with communication centers to be established among them;
- To build Arab national skilled capacities, train the law enforcement entities, advance the skills;
- 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.

Proposals at the Regional Level:

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 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;
- To put in place guidelines containing 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

Thank you!

Rouda AlAmir Ali

Rouda.alamirali@itu.int