Economic and Social Commission for Western Asia

"Personal Data Protection and Privacy in the context of emerging technologies"

Dr. Jeanane EL KHOURY

UNITED NATIONS
الاسكوا
ESCWA

Shared Prosperity **Dignified Life**

Outline

Overview

Practical Challenges and Legal Issues Raised in Arab Countries

Best Practices at the International Level:

- **UN / European Union**
- **Outside the region: France / Estonia / Mexico / UK**
- **From the region: UAE, KSA, Egypt**

Roadmap: How to enhance legal framework for the Personal Data Protection and Privacy in the context of emerging technologies

Conclusion

Introduction

- Digital public services: the most important Information and communication Technology (ICT) transformation in public sector.
- Public trust is the core of the digital transformation of Public sector.
- ICTs provide a modern way of government service delivery to the citizens.
- Arab Governments must be prepared.
- An ICT Legal and regulatory framework is crucial for successful digital implementation;
- **Need of Enforcement of laws, for improving trust in public digital services, Privacy and personal data protection...**

I. Practical Challenges and Legal Issues Raised in Arab Countries

- The ability to get the latest developed applications and software at reasonable price;
- 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 or/and costly Internet connection in some countries;
- The lack of a digital infrastructure in the Arab countries;
- The lack of information security in relation to some of the governmental institutions;

Legal and Regulatory Situation in Arab States:

- Few Arab States have adopted special law dedicated to personal data protection;
- Many Arab countries have no mechanisms to apply the elaborated rules.
- 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 **Cooperation countries (GCCs)** are among the top Arab countries that have paved the way for the digital area.

Legal Problems raised by the Artificial Intelligence (AI)

- The loss of human control over the machine;
- access to all data without any consideration of national laws and privacy or personal data,
- absence of a legal definition of artificial intelligence and the regulatory rules and professional ethics that govern it,
- “Whoever leads “artificial intelligence will rule the world, the third war will be a cyber war par excellence.”
- What actual degree of freedom will this artificial intelligence be granted to make its own decisions based on its analysis of the information?
- What is the applicable law?
- Can AI be held legally responsible for its decisions? Is it possible to apply international humanitarian law, the rules of which apply during wars and conflicts?
- Absence of legal frameworks, international rules and norms

Legal issues raised by the Blockchain:

- Legal methods of proving smart contracts, their nature and characteristics,
- Encrypted electronic signature on blockchains
- The electronic time stamp (authenticating the document and its timing),
- Proving the official document on the blockchain legally,
- lack of familiarity of legal status, and data protection and privacy considerations.
- Work of government agencies, eliminating bureaucracy, and trading money, digital currencies, stocks, and trading without an intermediary
- Difficulty of writing smart contracts, and not stopping their effects after they enter into force or change it, and the possibility of incorrect writing of code by developers..
- Attribution of the signed document to its owner, in order to clarify the extent of the need for a new system of proof that takes into account the peculiarities of this technology.

Legal Problems raised by data protection and privacy:

- Some Arab countries have adopted a special law to protect personal data
- In other countries there are only scattered texts, in the folds of separate legislation;
- Urgent need to protect privacy, and establishing the rules and foundations of the economic system of any country...
- Personal data has become a phenomenon of “Personal data trade”
- Exploiting consumer, employee, or customer data (name, phone numbers, email, and other social networking sites, home address, country...),
- Access to friends lists, family members, photos, events, traffic data, IP digital addresses, log files, GPS information, digital recordings, all with the aim of Processing without obtaining their consent,
- Many of laws in the Arab countries have been amended, particularly the commercial law, the criminal law and the law on civil procedure, in order to include the legal protection of information, data, intellectual property and digital documents, and to incriminate many computer-based acts committed..

II. Best practices
International organizations

UN: working groups have met at the United Nations affirmed that international law must be applied to cyberspace and set “behavioral standards” that ensure “responsible behavior”. The outcomes of the meetings of these working groups were adopted into resolutions of the United Nations General Assembly.

European Union:

It is known that the EU has taken several legal measures with the aim of protecting data, privacy, and cybersecurity, enhancing trust in the digital public services and **punishing giant technology companies when they violate European laws**.

1. **The Digital Services Act (2022)** is the most important in the field of the protection of the digital space against the spread of illegal content, and the protection of users’ fundamental rights.

2. The Digital Markets Act (August 2022) which consists of a set of rules that regulate the actions of so-called “gatekeepers” to ensure a fairer marketplace and increase availability of service options for users (individuals) and business users.

II. Best practices
International organizations (cont.)

EU GDPR

- The European Union's (EU) 2016 General Data Protection Regulation (GDPR) as an example of comprehensive regulation of data protection and privacy, requiring that personal data collection, storage, and use be processed lawfully, fairly and in a transparent manner..

- **The Council of Europe (CoE) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108, CoE 2018**
- duties to monitor, investigate and enforce compliance with individual privacy and data protection rights; their impact on individual privacy and data protection rights;
- The 2013 OECD Guidelines constitute a reliable and effective soft law instrument to promote and protect in efficient fashion the personal data of individuals.
- **The 2014 OECD Recommendation of the Council on Digital Government Strategies:** The first international legal instrument on digital government.

Countries' experience

1. Estonia

Estonia is one of the matured countries in the implementation of e-government and has a legal framework that supports the digital public services, and a successful e-court system.

It implemented its court information system in 2005 for all court types,

The Courts Act establishes a court information system which aims to organize the work of courts, collect statistics, collect and systematize decisions, and make them available to courts and the public. The Code of Criminal Procedure.

The Code of Civil Procedure and the Code of Enforcement Procedure, the Code of Misdemeanour Procedure, the Code of Administrative Court Procedure, and the Code of Civil Procedure enable the processing of digital documents and evidence in the specific procedure in the information system.

2. Mexico:

Mexican Government is harmonizing the legal framework in order to foster an environment of certainty and confidence favorable to the adoption and promotion of ICT inside and outside government.

The legal framework includes the following:

Constitutional Reform, National Digital Strategy, Advanced Electronic Signature Law, General Law for Transparency and Access to Public Information, Guidelines for Personal Data Protection.

Some agencies and entities in government in charge of designing the legal frameworks in specific areas, (Digital Government Unit, National Institute of Transparency and Access to Government information (INAI) …)

Countries' experience

3. United Kingdom:

A new version of the UK Data Protection and Digital Information Bill No. 2. (On 8 March 2023) aims to make provision:

regulation of the processing of information relating to identified or identifiable living individuals;

about access to customer data and business data;

about privacy and electronic communications;

about services for the provision of electronic signatures, electronic seals and other trust services;

for the implementation of agreements on sharing information for law enforcement purposes…

4. France:

Adopting many laws, decrees and decisions, on Data Protection on cybercrime, digital public administration, Electronic Interactions between Public Services Users and Public, on Electronic Communications and Audio-visual Communication Services on Trust in the Digital; on E-Invoicing Legislation Ordonnance (June 2014); Law on Programming 2018–2022 and on the Reform of (2019); on the Organization and Transformation of the Healthcare System (2019); on the Growth and Transformation of Enterprises (2019); on the Reduction of the Environmental Footprint of the Digital Sector (2021)…

French experience: legal and regulatory framework is a set of special laws and decrees that are integrated with each other, and with some amended laws, and are implemented by specialized and professional bodies, which can therefore be emulated.

Arab region

1. The United Arab Emirates (UAE):

enacted federal law n°1/2006 on e-transactions and e-commerce to protect the rights of online dealers and determine their obligations.

Federal Law n°2/2006 on Combating Cybercrimes, which is considered as a model law in the Arab countries...

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 …

Special law on the protection of its own data and lists that are in harmony with the EC directive on data protection (EC/46/95) and the directives of ESCWA and of OECD (Organization for Economic Cooperation and Development) (by The Dubai International Financial Center DIFC) ..

Dubai Law on data publication and exchange (open data law of October 17, 2015) has many of its terms dealing with the collection, legality and safe processing of data…

Launching the first court in the world that relies on "block chains" in 2018,

Developing logical models for smart contracts across the blockchain network.

Employing blockchain technology in notary transactions in the year 2021, and the certification service provided by the Ministry of Justice...

Allowing customers to submit transactions through a digital identity, whether they are inside or outside the country.

2. The Kingdom of Saudi Arabia

Adopting a comprehensive legal framework to support the digital transformation of public service production and delivery.

The Electronic Transactions Law, Telecommunications Act and the E-Commerce Law.

The “Personal Data Protection Law” (2022), which regulates the collection, storage, sharing and processing of personal data for everyone living in the Kingdom of Saudi Arabia, protecting the privacy of individuals, regulate the exchange of data, and ensure the privacy of personal data.

3. Egypt:

1. A new draft law supports providing all government services to citizens digitally, obliges government agencies to provide services to citizens digitally….

2. **the Personal Data Protection Law (No. 151 of 2020)** as a legislative breakthrough towards securing personal data for Saudi citizens, especially with existing legislation devoid of a legal framework regulating the protection of electronically processed personal data during its collection, storage or processing.

V: Roadmap “How to enhance legal framework for the Personal Data Protection and Privacy in the context of emerging technologies”

At the legal level, so far, no international or Arab law incriminates or penalizes the platforms and giant technology companies (as DSA EU), whose collect the big data and all personal data;

Developing a legal and regulatory framework within each country to define the controls for the use of Artificial Intelligence and to arrange the criminal responsibility resulting from the use of its applications;

Presenting all the relevant Arab laws that must be amended, all legal articles and all other legal and regulatory amendments, as well as presenting recent provisions related to public digital services;

Legal frameworks should include sufficient penalties for unauthorized access, use or alteration to personal data;

Enforcing 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 platforms and 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.

Legal Framework for banking services: Several banking and financial laws should be amended to form a safe and stable banking system, and to control the data and prevent any fraud or misuse.

Executive Proposals:

- **At the judicial level**, Arab courts have to deal with digital cases and e-proof
- Implementation of e-court system which will present many improvements to the daily processes…
- The participation of the public policy makers in the States in drawing up local policies that stress the importance of digital public services and of catching up with the technological development in consistence with the national priorities.
- Help Arab governments adopt more strategic approaches for a use of technology and data that spurs more open, participatory and innovative governments;
- Participation of all stakeholders and the entire public sector (Ministries and public administrations), in enhancing the trust in public digital services;
- Strengthening the institutional capacities of the Arab government and supporting it with local and foreign expertise to develop legislative and regulatory systems, and to assess and manage risks;
- Raising the awareness of decision makers about the importance of public digital services for sustainable development.

Regionally

- An Arab Safe Harbor Agreement
- 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.
- participation of all concerned stakeholders in establishing an Arab regulatory and legislative structure of digital public services such as policymakers, 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.
- take advantage of best practices and successful experiences at the international level.

Conclusion

- A relevant ICT regulatory framework is essential in this transformation process to ensure the validity of electronic transactions and guarantee the proper usage of technological tools
- Digitization brings new challenges to the public sector.
- Security and trust are also necessary to ensure secure online access and reliable exchanges of data and information, and to reap the enormous social and economic benefits of connectivity.
- Many Arab States have launched projects and strategies to adopt the Digital public services 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.
- the implementation of the digital public services is the result of a collaborative effort, of talks with experts, industry and academics, legislators, civil organizations and citizens (Stakeholders).
- priorities of the government work system in the present and the future are to fulfill the aspirations of the citizen, build on the achievements made, and maintain the sustainability of growth.

UNITED NATIONS
الاسكوا
ESCWA

Shared Prosperity Dignified Life