Regional Workshop

"Policies on data privacy and cybersecurity"

Tunis, 5 & 6 December 2016

Report

Upon the initiative of the International Telecommunication Union (ITU Arab Regional Office), and in partnership with the Arab Information and Communication technology Organization (AICTO), in collaboration with El Ghazala Technopark in Tunis, and under the auspices of the Tunisian Ministry of Communication Technologies and Digital Economy, the regional workshop on "policies on data privacy and cybersecurity" was held on 5 & 6 December 2016 at El Ghazala Technopark, in Tunis.

82 participants from different Arab and African countries, namely Burkina Faso, Comoros, Mauritania, Palestine, Saudi Arabia and Tunisia representing the public sector, (ministries and public institutions), the private sector, international and regional agencies and organizations (UNDOC, ISOC) and the civil society (universities and professional associations).

The scientific program was run by eminent international experts, namely from the National body for the protection of personal data (INPDP- Tunisia) who outlined the importance of many issues related to the protection and preservation of personal data, and its impact on the setting up of a transboundary trust space.

With the sporadic development of ICT applications and services, and the network convergence towards the Internet, personal data has acquired a major importance. Indeed, the easy access to telecom infrastructures has largely contributed to the intrusion into the individual privacy.

'Personal data' means any information which allows to directly or indirectly identify a person. Such data is part of the individual personality, and therefore belongs to him/her and cannot be marketed.

If personal data is communicated to structures or companies for well determined services, it doesn't imply property transfer and the data processing unit is responsible for the security and safety of this data not to be disseminated.

This personal data has become very important within the digital environment and digital society due to its great economic value. And the "mega-bases of behavioral data " pave the way to efficient and profitable way to market through the use of big data and cloud computing technologies. The new technologies such as the Internet of Things and M2M are accelerating this trend.

Thus, the personal data processing has become a market opportunity that offers many services and contribute to the creation of new careers.

This processing can have as a target to cross data, set up individual profiles, make behavioral consumption, voting forecasts with an impressive reliability and truth. These behavior forecasts are very often achieved without informing the concerned individuals.

Public structures also need to collect a growing group of citizen data in order to create guidance boards that will enable them to plan and design adequate public policies to meet the needs of the community.

With the rise of terrorism and cybercrime, security services also seek to develop large-scale control systems able to secure the cities and the state borders. The processing is even more sensitive because the constraints of the real time and reliability become more crucial.

Many experiences have shown that cyber-criminals and terrorists are taking advantage of the presence of personal data preservation mechanisms to build cover channels through which they can communicate without tracking and prosecution by the authorities. The balance between the protection of personal data, the legal data interception and digital forensics should therefore be perceived as one of the issues to be dealt with by the legal, technical and scientific community to find out adequate solutions.

This mass collection of personal data as well as its processing require therefore the setting up of warranties for the benefit of the persons concerned so that their personal data will be handled with respect to their privacy. This is the essential condition that would preserve the source of this data by preserving the confidence of the person who processed the data. The standards for personal data protection are becoming universal. Indeed, the international community through the United Nations decided to create the position of ‘Special Rapporteur’ dedicated to the right of private life protection.

Recommendations

The works of this two-day workshop were concluded by the following recommendations:

- Personal data processing for the private sector companies and governments should depend on the sense of confidence. Confidence can only be available through establishing a relationship between the two parties who have a sound knowledge and culture. This basic requirement can be done through formal education at an early age to educate individuals on the importance of this issue, and inform them about their relevant rights and the obligations of the people responsible of the processing.

- Invite Arab countries to set up the legal framework that protects the individual personal data (to this date only 3 out of 22 Arab countries have the legal framework whereas only only 2 of them have the relevant authorities).

Through this legislation we can identify the obligations of persons who are responsible of the processing, namely :

- Declaration or authorization request.
- Obtaining prior approval.
- Purpose respect.
- Data securing.
- Data updating.
- Carefully connecting and transferring data.

The law should also guarantee to the concerned people the rights to process their personal data:

1. Opposition right.
2. Right to direct and indirect access.
3. Rectification right.
4. Oblivion right.

The legal framework should create an independent body for personal data protection in accordance with the Paris standards and convention 108 of the Council of Europe.

- Arab countries are invited to make further efforts to create an Arab Convention for the protection of personal data which would take into account the relevant international standards.

- Public authorities as well as the civil society components in the Arab region are invited to create a space for exchange, awareness and cooperation on this issue by launching the "Arab Network for the Protection of Personal Data".
- Public authorities are invited to :
  - Speed up their country's adhesion to the Convention 108 of the Council of Europe and the African Convention on the protection of personal data.
  - Set up through independent certification authorities, labels and certifications related to personal data to the protection.
  - Create a mechanism for external audit performed by qualified experts assessing the level of protection ensured by public and private structures.
  - Set high financial penalties to deter violations of individuals' rights in protecting their personal data.
- Invite regional organizations and non-governmental organizations to support the Arab civil society and media to launch individual awareness programs on the dangers arising from a lack of vigilance related to the processing of personal data programs, namely:
  - Modify the individual's behavior into a responsible citizen and aware of the dangers facing his/her privacy.
  - Adapt the use of technology to the need and educate citizens on how to protect data by creating multiple profiles and e-mail accounts or on social networks.
  - Advise individuals to choose anonymity to protect his privacy and avoid publishing personal pictures or all aspects of their private life.
  - The use of encryption technologies in personal data communication and exchange transactions.
- •The confidentiality issues on the Net are systemic involving different parties (economic, social, political, technical, personal,..) : isolated solutions are unlikely to succeed.
- • Comprehensive approach should be applied and the issue of privacy addressed from different aspects with appropriate measures.
- • Encourage the adoption of the principles of Privacy By Design (PBD) and the ethic data management .