



## “Cyber Crime” Insights from the Egyptian Laws

Judge Dr. Ehab Elsonbaty

[ehabelsonbaty@hotmail.com](mailto:ehabelsonbaty@hotmail.com)

[ehabelsonbaty@yahoo.com](mailto:ehabelsonbaty@yahoo.com)

COE Conf - June 07 - Dr. Elsonbaty

1

## Topics of discussion

- Current status of cyber crime legislation in Egypt.
- Reforms underway and key questions.
- Correspondence of the draft law to the Council of Europe Convention rules.
- Conclusion.

COE Conf - June 07 - Dr. Elsonbaty

2

## Backgrounds 1

- Egypt is a civil law country.
- every thing should be regulated /codified.
- green / blue paper theory.
- Not used to codes of conduct,
- Nor implementation guidelines.

COE Conf - June 07 - Dr. Elsonbaty

3

## Backgrounds 2

- **Regulating means:**
- Making computers, networks, ..etc:
  - more functional,
  - less complicated and
  - most importantly as safe and reliable as possible.
- What to do, what not to do and how?
- Creating norms of behaviour.

COE Conf - June 07 - Dr. Elsonbaty

4

## Backgrounds 3

- How is the ICT, mainly Telecommunications and INTERNET regulated in Egypt.
- Law No. 10/ 2003 issuing the Telecommunication Regulation Law.
- Copy rights Law 80/2002.
- Electronic Signature 10/2004.
- Decree No. 109 Of The Year 2005 Dated 15/5/2005 Issuing The Executive Regulations.

COE Conf - June 07 - Dr. Elsonbaty

5

## E- Laws

- The only “Electronic law “ is the E-signature Law.
- **Work in progress for:**
- E - Commerce Law,
- Cyber Crime Law,
- E – payment Law and
- Data Protection Law.
- Recently a Consumer Protection Law was passed 67/2006.

COE Conf - June 07 - Dr. Elsonbaty

6

## Overview of Electronic Signature Law 1

- Articles 14 – 18 explain the legal value of electronic writing and electronic signature, its weight of proof, its ability to prove obligations and rights.
- If the criteria are met the electronic writing is considered as the paper one and has the same weight of proof.
- The electronic document was also explained.
- The electronic signature will have the same proof evidence as traditional signature by giving credibility to the content of the electronic writing it is signed with.

## Overview of Electronic Signature Law 2

- **ARTICLE 18:**
- The electronic signature, electronic writing, and electronic documents shall enjoy their conclusiveness in providing evidence in case they fulfil the following conditions:
  - a) Linkage of the electronic signature exclusively with the signer;
  - b) Control of the signer exclusively on the electronic medium;
  - c) The possibility of uncovering any modification or replacement in the data of the electronic document or electronic signature;
- The executive regulations of the present Law shall determine the technical and technological regulators necessary therefore.

## Crimes punished by the Electronic Signature Law 1

- **ARTICLE 23:**
- Subject to any stricter penalty prescribed in the Penal Code or in any other Law, a penalty of imprisonment and a fine of not less than ten thousand Egyptian pounds and not exceeding one hundred thousand Egyptian pounds or either penalty shall be inflicted on:
  - a) Whoever issues an electronic ratification certificate without obtaining a license for exercising the activity from the Authority;

## Crimes punished by the Electronic Signature Law 2

- b) Whoever damages or vitiates an electronic signature, a medium, or an electronic document, or fakes something of that by fabrication, modification, alteration or in any other way;
- c) Whoever uses a vitiated or faked electronic signature, medium, or electronic document while being aware of this;
- d) Whoever violates any of the provisions of articles (19, 21) of the present Law;

## Crimes punished by the Electronic Signature Law 3

- e) Whoever manages by any method to obtain without due right an electronic signature, a medium, or an electronic document, or penetrates that medium, obstructs it, or inactivates the performance of its function;
- Whoever Violates article (13) of the present Law shall be liable to a fine penalty of not less than five thousand pounds and not exceeding fifty thousand pounds.

## Crimes punished by the Electronic Signature Law 4

- In case of recidivism, the penalty prescribed for these crimes shall be doubled in its minimum and maximum limits.
- In all cases, the court shall rule the publishing of the conviction sentence in two daily widespread newspapers and on the open electronic information networks at the expense of the convict.

## Crimes punished by the Electronic Signature Law 5

- **Article 24:**
- The officer in charge of actual management of the violator juridical person shall be liable to the same penalties prescribed for the deeds committed in violation of the provisions of the present Law, if his default on the duties imposed on him by such management has contributed to the occurrence of the crime, while being aware of this.
- The juridical person shall be jointly responsible for executing the financial penalties and compensations awarded by the court, if the violation has been committed by one its workers in the name and the interest of the juridical person.

## Draft Law on “Regulating the protection of Electronic Data and Information and Combating Crimes of Information“

- Discussed in the parliament.
- General overview.
- The compliance of the Draft Law with the requirements of the Council of Europe Convention on Cyber crime.

## Generally:

Three different comparisons may be made:

- For article which exists in the Convention and the law,
- For articles which exists in the Convention and needed to be reflected in the law,
- For articles exists in the law but does not contradict with the Convention.

## definitions

- Corresponding regarding: "computer system“, "computer data“ and "traffic data“.
- Just minor review suggested regarding “service provider” as it seem narrower in the law (Controller of the electronic data and Information + Controller of the electronic information system)
- than the convention in a way that may not cover access provider who enable users to use the Internet.

## General comment on articles from 2 – 31:1

- There is an obvious overlapping through the whole text between cyber crimes and data protection issues.
- The lines between the two subjects are not clear in the draft law, a matter that the law makers should have considered.
- Establishing a data protection Commission has exhausted more than 25% of the draft to the extent that cyber crimes may sometimes be marginalized.

## General comment on articles from 2 – 31:2

- The previous mentioned overlapping has resulted in having articles touching on cyber crime from a side and data protection from the other side.
- For example article 5 (substantial conditions for the protected data and networks) article 8 (admissibility of e- evidence in criminal matters), articles 10 + 14 (availability of data which is a substantial sabotage crime), article 12 (searching networks and data safeguards - law enforcement and procedures issues)....

## General comment on articles from 2 – 31:3

- Building a comprehensive legal framework to Regulate data protection is a very important target,
  - which,
- should be also true regarding cyber crimes.

## Criminalisation issues 1

- 2 Illegal Access 33 Corresponding
- 3 Illegal Interception Not covered
- 4 Data Interference 34 Review necessary
- 5 System Interference 34 Review necessary
- 6 Misuse of Devices 32 Review necessary
- 7 Computer-related Forgery 35 Review necessary

## Criminalization issues 2

- 8 Computer-related Fraud Not covered
- 9 Child Pornography 37 Review necessary
- 10 Copyright Infringements Not covered
- 11 Attempt 38 Corresponding
- 11 Aiding or Abetting Not covered
- 12 Corporate Liability 45 Review necessary
- 13 Sanctions and Measures Review necessary

## Criminalisation issues 3

- 14 Scope of Procedural Prov. 40 Review necessary.
- 15 Conditions and Safeguards 40 Review necessary.
- 16 Expedited Preservation 40 Review necessary.
- 17 Partial Disclosure 40 Review necessary.
- 18 Production Order 40 Review necessary.
- 19 Search and Seizure 40 Review necessary.

## Criminalisation issues 4

- 20 Collection Traffic Data 40 Review necessary.
- 21 Interception Content Data 40 Review necessary.
- 22 Jurisdiction Not covered.

## International Co – operation 1

- The mere fact appearing from the Egyptian Cyber Crime Law that it does not have a designated part for the international co-operation which is a basic part of the Council of Europe Convention on Cyber Crime, however, this should not lead to a prejudice against the Egyptian legal system.
- There are many rules governing international co-operation in criminal matters, analyzing them in the light of the Convention's rules clarifies the exact status of international co-operation in cyber crime issues in the Egyptian law.

## International Co – operation 2

- 23 General Principle,
- 24 Extradition,
- 25 Mutual Assistance,
- 26 Spontaneous Information,
- 27 Absence Int. Agreements,
- 28 Confidentiality.
- Not covered (but covered by other rules for international co-operation).

## International Co – operation 3

- 29 Exp. Preservation,
- 30 Partial Disclosure,
- 31 Accessing Store Data,
- 32 Trans-border Access,
- 33 Collection Traffic Data,
- 34 Interception Content Data,
- 35 24/7 Network.
- Not covered

## Conclusion 1

- The Draft Law is with regard to a large number of provisions – especially regarding the substantive criminal law provisions – fulfilling the requirements of the Convention on Cyber crime.

## Conclusion 2

- Some provisions do not yet meet the requirements of the Convention on Cyber crime.
- The analysis points out these provisions as well as those provisions, where the compatibility with the Convention on Cyber crime is uncertain.



## Cyber Crime

### Insights from the Egyptian Laws

- *Many thanks for your attention.*
- *Any questions?*

Judge Dr. Ehab Elsonbaty  
[ehabelsonbaty@hotmail.com](mailto:ehabelsonbaty@hotmail.com)  
[ehabelsonbaty@yahoo.com](mailto:ehabelsonbaty@yahoo.com)