Expert Meeting on

CYBERLAWS AND REGULATIONS FOR ENHANCING E-COMMERCE: INCLUDING CASE STUDIES AND LESSONS LEARNED

25-27 March 2015

Sudan Paper

Presented by

Sudan Ministry of Trade

SUDAN PAPER

Nowadays the world is open to adopt E-commerce which is the digital use of information technology for completing administrative transactions, as such security has become a more critical factor in ensuring information and data privacy and protection.

E-Transaction Laws

This part of the paper underlines the main national legislations in Sudan that addresses E-transactions.

- **Civil transaction Act 1984** provides legal basis for e- commerce. The Act clearly recognizes contracts and financial transactions finalized through modern technology facilities. The Act provides that such transactions have the same legal effect as those done on paper by the principle or an agent. The Act does not insist on a typical form for the parties to express their wills.

- **Electronic Transactions Act 2007:**

  - The cornerstone piece of legislation addressing E-commerce.
  - It mentions for the first time "electronic contract" which has the same legal effect as other traditional type of contract.
  - It precisely recognizes the electronic message as a means for expressing the parties wills and for offer and consent.
  - It introduces electronic digital signature as having the same legal effect as paper hand signature.
  - It recognizes equal legal effect for electronic messages as that of material evidence (papers or otherwise). The effect can't be denied just because they are produced in an electronic form.

- **The Informatics Offences Act 2007:**

  Enumerates crimes and illegal acts, which are:

  - Threatening the privacy of the parties of E-transaction or aiming at causing illegitimate profit to someone or inflicting unauthorized loss to any of the transaction parties.

- Entry of informatics sites to cancel, destroy or change, to top, pick up or obstruct messages. To impede, jam or disturb access to services or entry sites, programs or source of data information.
- Obtaining digits or data or credit cards
- Money laundering.

These crimes are punishable with imprisonment for different terms not exceeding 10 years, fine or both.

- **The Money Laundering Combating Act 2014:**
  - The Act provides for precautionary measures to prevent money laundering operation. It underlines the duties of financial and non- financial institutions as well as the establishment of the Investigation Unit.
  - The Act also provides for penalties such as imprisonment for a term not exceeding ten years and not less than five and fines as well as confiscation and other administrative sanctions.

Electronic Fund Transfers:

- The Regulation on the Electronic fund Transfers 2013 identifies money transfers through (i) point of sale (pos) terminals (b) automated teller machines (ATM), (c) TV, Internet and other communications channels,(d) telephonic instruments, including mobiles. (e) debit cards, (f) card- based and network – stored value products.
- The Regulation gives details on the time of receipt of payment order, it's irrevocability, authorization of transfers, erroneous payment, unauthorized use and liability in case of device malfunction.

<u>Payment system</u>

- **Regulating payment system:**

Article 6 of the Central Bank Act of **2002** entitles the Central Bank to organize and supervise the payment systems whether electronically or manually.

In **2013** the first regulation in that direction was adopted:

(i) A national payment system managed by the Central Bank of Sudan was established.

(1) The Regulation defines payment system as (i) services associated to sending, receiving and processing of orders of payment or transfer of money in domestic or foreign currency.

That includes any system or arrangement for the processing, clearing or settlement of funds.

(2) Issuance and management of payment instruments.

(3) Arrangement and procedures associated to those systems.

(4) Payment service providers, including system operators, participations, and third party acts as an agent or by way of outsourcing.

(ii) The Regulation recognizes payments whether tangible or intangible that enable a person to obtain money, goods or services. These may be cheques presented electronically by the transmission of image, digital representation or electronic funds transfers (credit or debit) through electronic means.

That includes point of sales, automated teller machines, transfers initiated by telephone, Internet, payment card or other devices.

(iii) The rules also adopt truncation as a means of settlement process in which the physical transfer of a paper is substituted by the exchange and storage of its image and electronic information.

(iv) The Regulations recognizes magnetic or any tangible and intangible device such as SIM card or software, stored monetary value as approved by the Central Bank. However stored money must always reflect corresponding amount of money deposited within a bank account as established by the Central Bank. Electronic money may also be in a form of stored value–value cards.

Another type of cards is payment card which includes card, coupon book or other device including code or any other means of access to an account to obtain money or make payment.

(v) The Regulation has numerated types of electronic instruments which are recognized by the law. It also provides for clearance and settlement of payments through the system.

Consumer protection

Legal provisions aiming for the protection of consumers online are scattered over various legislations.

- The Civil Transaction Act 1984 and the Electronic Transactions Act 2007 provide for:

- Recognizing the validity of electronic contacts as well as equating their legal cogency with paper and other legal dealings.
- Recognizing the digital signature and it's binding legal effect.
- Non-discrimination against electronic instrument just because it's introduced in an electronic device.
- The Electronic Transaction Act 2007 underlines the secrecy of information and the legal duty of non-disclosure of such information.
- The Regulation on E- Fund Transfers confirms the privacy of the related information, affairs or the account of a customer, reception of payment, the authorization of transfers, the erroneous payment orders and the liability thereof.
- The Regulation also imposes on the customer the duty to notify any error in his statement of account or possible unauthorized transaction, misuse, loss or theft.

A customer is under a duty to not disclose to any person the security access code of his card or any electronic device.

- The Regulation also gives the customer the right to a refund in cases where the authorization did not specify the exact amount of the payment transaction or it exceeded the amount the payer could reasonably have expected.
- Standard terms and conditions of carrying out E transfer should be available to customers, certain information are also required if payment is made by voice communications.
- A formalized procedure for the lodgment of complaints by customers should be provided by the service provider. That includes appropriate procedures for the investigating and resolution of complaints and a time table for settlement of disputes. Copies of investigations shall be made available to the customer.
- A customer should be informed about his right to appeal against the outcome of a complaint and that he has the chance to refer the Central Bank.
- No agreement between a customer and a service provider is allowed that contains any provision which constitute a waiver of a customer's rights. However an agreement that provides greater protection is allowed.
- A customer may resort to the mechanisms specified by law for customer rights protection, such as the special attorney general office established for that purpose. However for seeking rapid resolution to disputes the law enumerated other available mechanisms with the service provider or the Central Bank. The

Sanction Committee established by the Bank Business Organization Act 2004 also has jurisdiction to resolve customer's disputes.

Cybercrime prosecutors and specialized police department have been establish as stated in the Electronic transactions law 2007. Their main objectives are to deter cybercrime and enforce the law, working in coordination with the National Communications Corporation and the National Intelligence and Security Agency. During recent years the Cybercrime prosecutor has dealt with various types of cases which can be classified as follows:

- Crimes related to E-money transfer.
- Website attacks.
- Social Media Networks and Applications.
- Mobile Networks misuse.

One of the major recent cases covered by the Cybercrime prosecutor is related to electronic money transfers. The victim was a Sudanese company that used to transfer money to its trade partner abroad, but its correspondence had been interrupted and misused by a third party who was able to divert 500,000 Euro into his private account. The prosecutor initiated the case and communicated with the authorities in the other country via official channels, asking them to collaborate, but because the suspect's country of residence doesn't have Exchange of Criminals Agreement with Sudan, the suspect could not be extradited, also the prosecutor was unable to present in that country judicial system. They provide the company with the formal documents needed to complete the litigation abroad. It is worthy of mention that the sentence for such a crime is 5 years in prison as stated in the 2007 Law.

Sudan has developed an Information Security strategy based on International Telecommunication Union (ITU) framework on cybersecurity, programe 3 on cybercrime fighting procedures and ITU-IMPACT global cybersecurity agenda.

1. The ITU framework is a management framework for organizing National efforts on cybersecurity, which is composed of 5 pillars as follow:

   - Developing a National Strategy for Cybersecurity;
   - Establishing National Government–Industry Collaboration;
   - Deterring Cybercrime;
   - Creating National Incident Management Capabilities; and
   - Promoting a National Culture of Cybersecurity.

2. "ITU Cybersecurity Work Programme to Assist Developing Countries 2007-2009" which is known for short as Programe 3 has the following elements:
   - Developing National strategy
   - Establishing a deterring legislations

- Establish incident control capability
- Combating SPAM
- Bridging Standardization gap between developed and developing countries
- Develop cybercrime measures
- Cybersecurity regional and international cooperation
- Conducting research and training.

3. The GCA is built upon the following five strategic pillars, also known as work areas:
   - Legal Measures
   - Technical & Procedural Measures
   - Organizational Structures
   - Capacity Building
   - International Cooperation

Taking all the above into consideration, Sudan has built its own cybersecurity approach which has led to a number of important achievements.

Sudan has adopted a number of important e-crime legislations for fighting e-crimes including e-commerce crimes, the most important ones are:

- E-Crime Law - 2007
- Informatics offences (Combating Act) 2007

Meanwhile, Sudan has officially established Sudan Computer Emergency Response Team (Sudan–CERT) by a generous initiative of National Telecommunication Corporation; the telecom regulatory authority in Sudan, as a national ability to enhance Information and Network Security all around Sudan. Sudan-CERT vision is "For a Safe Online Community".

One of the important ongoing activities of the center is the awareness programs that are conducted to the Internet users especially school children, with an objective of achieving Internet safely.

Last year – 2014 – Sudan-CERT dealt with 150 e-crime cases. Social media crimes made up about 85% of the total number of cases. These include impersonation and identity theft, distortion, blackmail, abuse, offense acts and others. The other types of crimes are laptop and mobile theft, phishing, web defacements, inappropriate content, child abuse and others.

In 2014 Sudan-CERT investigated a number of e-commerce cases where thousands of US dollars were stolen, Sudan-CERT with the help of e-crime police and ISPs have been able to recover some of the money.

To fight Cybercrime it is a must to build strong cooperative relations regionally and internationally, Sudan-CERT is a member of important organizations and groups, for instance:

- ITU
- IMPACT (International Multilateral Partnership Against Cyber Threats)
- OIC-CERT (Organization of Islamic Cooperation CERTs)
- Africa-CERT
- APWG (Anti Phishing Work Group)
- COMESA
- Etc

Also Sudan-CERT has important bilateral relations with many National CERTs all around the world.