CHALLENGES FACED REGARDING CYBER CRIME AND THE RULE OF LAW IN CYBERSPACE FROM THE PERSPECTIVE OF A PROSECUTOR IN GHANA

BY
MRS. YVONNE ATAKORA OBUOBISA
AG. DIRECTOR OF PUBLIC PROSCUTIONS, MINISTRY OF JUSTICE AND ATTORNEY GENERAL DEPARTMENT, GHANA

LEGISLATIVE FRAMEWORK

- Robust legislative framework in place to deal with cyber offences.
- Electronic Transactions Act, 2008 (Act 772): mainly sets out the cyber crimes
- Electronic Communications Act, 2008 (Act 775)
- Mutual Legal Assistance Act, 2010 (Act 807)
- Data Protection Act, 2012 (Act 843)
- Criminal Offences Act, 1960 (Act29)
- Criminal and other Offences Procedure Act, 1960 (Act 30)

LAW ENFORCEMENT INSTITUTIONS

- Economic and Organised Crime Office (EOCO)
- Ghana Police Service (CID/Cyber crime Unit)
- Bureau of National Investigations (BNI)
- National Security Council Secretariat

PROSECUTING AND JUDICIAL AUTHORITIES

- Prosecution Division of the Ministry of Justice and Attorney General's Department,
- EOCO with the Fiat of the Attorney General
- Judicial Authority : cyber crime cases can be prosecuted both in the high court and the lower courts.
- The Police Prosecutors: prosecute in the circuit courts.
- The CJ has set up the financial division of the high court to speedily try cyber crime cases manned by trained Judges.

CYBER CRIME OFFENCES IN GHANA

- Stealing
- Appropriation
- Representation
- Charlatanic advertisement
- Attempt to commit crimes
- Aiding and abetting
- Duty to prevent felony
- Conspiracy
- Forgery
- Intent
- Criminal Negligence
- Access to protected computer
- Obtaining electronic payment medium falsely

CYBER CRIME OFFENCES IN GHANA

- Electronic Trafficking
- Possession of electronic counterfeit-making equipment
- General offence for fraudulent electronic fund transfer
- General provision for cyber offences
- Unauthorised access or interception
- Unauthorised interference with electronic record
- Unauthorised access to devices
- Unauthorised circumvention
- Denial of service
- Unlawful access to stored communications

CYBER CRIME OFFENCES IN GHANA

- Unauthorised access to computer programme or electronic record
- Unauthorised modification of computer programme or electronic record
- Unauthorised disclosure of access code
- Offence relating to national interest and security
- Causing a computer to cease to function
- Illegal devices
- Child Pornography
- Confiscation of assets
- Order for compensation
- Ownership of programme or electronic record
- Conviction and civil claims

CHALLENGES

1. Challenge in accessing electronic evidence : lack of cooperation from service providers.

- Section 103 of the ETA mandates service providers to keep logs and records of the

    a. Name

    b. Electronic source and destination address

    c. billing records if any

    d. duration of service to a subscriber or customer

    e. types of services and related logs of the subscribers

    f. Activities which takes place on its electronic platform as may be reasonably appropriate for a period of twelve months.

In spite of this provision in the law, it is not enforced because many law enforcement officers are not aware of this provision and the powers they have to demand compliance from service providers.

CHALLENGES

2. The complex nature of investigation required to gather evidence to prosecute cyber cases. Currently, in Ghana we are faced with several cases of revenge porn and use of internet to malign healthy businesses.

Examples: several incidence of attacks on young women with the use of internet.

Also, there are reported cases of the internet being used to harm competitive businesses.

Here, the difficulty is in tracing of the primary source of the information. The Cyber Crime Unit and other Law Enforcement Units are often unable to get to the source of the information even within the country and it is even more complex where the service provider is outside the Jurisdiction and we would have to rely on mutual legal assistance request. This often happens when the information is spread through social media platforms like whatsapp.

CHALLENGES

3. Improper handling of electronic evidence - Some of our investigators lack experience in the gathering of electronic evidence in compliance with our admissibility rules. This leads to very vital evidence being rejected by the courts.

4. Chain of custody – in cases where electronic evidence moves among various institutions it is essential to maintain proper custody to ensure admissibility in Court.

CHALLENGES

5. Unwillingness of witnesses to testify for fear of being stigmatised or losing clientele. E.g..

a. Banks, Automobile Industry and Insurance Companies are often not willing to pursue cases when the face cyber attacks for fear of losing clientele and the negative image their companies might face.

b. Women who face forms of cyber bullying or revenge attacks are unwilling to testify because of the stigma attached to such cases. Often Parents, Religious Leaders and even sometimes Community Leaders try to settle such cases out of Court.

CHALLENGES

6. Long delays associated in gathering evidence. This is normally the case where we deal with internet facilitated bank frauds where the attacks on the software of the bank happens from outside the Country. Investigations and prosecutions involve cooperation from other Countries and this often takes a lot of time in the gathering of evidence.

7. Law Enforcement Institutions have inadequate digital forensic tools to gather electronic evidence. Investigators sometimes have to fall on private cyber forensic companies for assistance in conducting digital forensics.

CHALLENGES

8. It is a fairly new area in our criminal Jurisprudence and so we lack enough precedents to resort to in prosecuting these cases.

Not too many of the Judges have been trained to handle cases on cyber crime and this poses a challenge.

THE WAY FORWARD

- Accession to the Budapest Convention is not a magic wand. It does not guarantee that all our cyber challenges will be solved overnight. It does however provide a platform to build synergies, cooperate with member Countries and commit communally to provide stronger resistance to cyber crime.
- Working together we will weaken the front of organized cyber crime activity in our individual Countries.

- THANK YOU