Policing Cybercrime and Protecting Human Rights: Ensuring an Appropriate Balance through Legislation

Dr. Nnenna Ifeanyi-Ajufo

Senior Lecturer of Law and Technology, Swansea University, United Kingdom/
African Union Cyber Security Experts Group

Human Rights and Cyberspace

"State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms set forth in the Universal Declaration of Human Rights and other international instruments." - The United Nations Group of Governmental Experts (GGE) on Advancing responsible State behaviour in cyberspace in the context of international security.

- Countries are increasingly declaring cybersecurity and cyber attacks against their governments and citizens as a national security threat.
- Policies and legislation that focus on policing cybercrime can also limit human rights.
- One of the key underlying principles for any cybercrime legislation is that it should have as a fundamental objective the protection of human rights.
- In promulgating Cybercrime legislations and policies, governments must remember their human rights obligations and uphold the provisions of Human Rights Instruments

Cybersecurity and human rights are interrelated.

THE NIGERIAN SITUATION

- The Economic Community of West African States (ECOWAS) has ordered the government of Nigeria to repeal or amend the provisions of its cybercrime law which it says violates the rights of expression of Nigerians with the enactment of Section 24 of the Cybercrime Act, 2015.

Determining whether an interference with human rights is to be justifiable.

States must enact cyber security laws that take into account their constitutions and international conventions in relation to human rights.

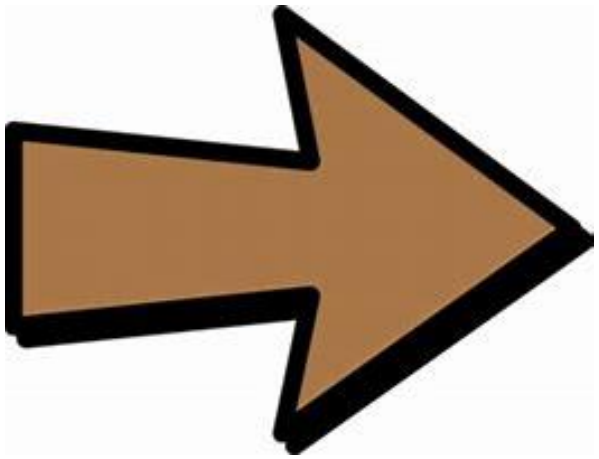
These conditions are:

- (i) the interference must be in pursuance of a legitimate aim;
- (ii) it must be in accordance with the law; and
- (iii) it must be necessary in a democratic society.

If the State cannot satisfy any of these conditions, there will be a finding of a violation of human rights.

It is necessary that the law contain provisions concerning the precise circumstances under which rights may be breached and for what purpose.

A general power to take steps necessary for the policing of cybercrime should never be a sufficient basis to infringe on human rights. Such measures must have a sufficiently clear basis in the national law.



MULTISTAKEHOLDER INVOLVEMENT IN POLICY AND LEGISLATION PROCESSES

- While governments mostly create and develop cybersecurity policies and initiatives, it is important to consult technical experts, private businesses, academia and civil society for recommendations.
- Private sector companies, including ISPs and the IT sector are crucial because of their role in creating and maintaining the technologies on which cybersecurity issues arise and sometimes profit from human rights infringing cybersecurity policies.
- The technical community has the technical expertise and understanding of the Internet and is often cited by governments when developing cybersecurity policies.
- Civil society is uniquely positioned to advocate for cybersecurity policies based on a human rights approach

Thank you, for your attention

Merci pour votre attention

We must consistently ensure an Open, Safe and Secure Cyberspace which allows for Human Rights guarantees.

شكرا لك على انتباهك

Obrigado pela sua atenção