CYBERSECURITY LAW AND REGULATION

Uchenna Jerome Orji

Barrister and Solicitor of the Supreme Court of Nigeria
LL.B (Hons) (University of Nigeria), BL (Nigerian Law School),
LL.M (University of Ibadan)

Dedication

To Sir & Lady Moses Orji (KSJ).

To my siblings:

Ify,

Ngozi,

Tobechukwu, and;

Ugochukwu.

To Emmanuel Orji;

And;

To the living memory of Barrister Orji Jerome Arochukwu
(1973- 2009).
"*…And even in our sleep, pain that cannot forget, falls drop by drop upon the heart, against our will comes wisdom to us by the awful grace of God*".
Agamemmon of Asechylus.

CYBERSECURITY
LAW AND REGULATION

Uchenna Jerome Orji

ISBN: 9789058508577

Published by:

Wolf Legal Publishers (WLP)
P.O. Box 31051
6503 CB Nijmegen
The Netherlands
Tel: +31 24 355 19 04
Fax: +31 84 837 67 00
E-Mail: info@wolfpublishers.nl
www.wolfpublishers.com

"Cybersecurity looms as the 21st century's most vexing security challenge…Technology continues to race ahead of the ability of policy and legal communities to keep up".

John Edwin Mroz,
President and CEO EastWest Institute.

Preface

During the 20th century, technological advances brought about the convergence of telecommunications and computer technologies. This signified the beginning of an era known as the *information age*. The information age is characterized by the rise of digitalization which basically implies a technological shift from analog and electro-mechanical technologies to digital technologies. A very distinctive feature of the information age is the continuous integration of computer and digital communications technologies in virtually all aspects of life and critical services that support modern societies and the tendency towards "connecting everything to everything". This has given rise to the emergence of the information society. However, the emergence of the information society as a result of the integration of computer and digital communications technologies in all aspects of life has also redefined traditional notions of security. The security of digital data, computers, digital communications technologies and information networks now have an overwhelming influence on almost all aspects of life and society including the global economy. Thus, with the emergence of the information society, malicious conducts against information systems such as computer systems and networks now have the potential of affecting individuals, countries and the global economy in ways previously unimagined. The most critical challenges of the information society have been the security of digital data and information systems and the prevention of the malicious misuse of information communications technologies by criminals, terrorist groups, or state actors. Measures to address these security challenges of the information society have given rise to a new concept known as "cybersecurity". Cybersecurity seeks to promote and ensure the overall security of digital information and information systems with a view to securing the information society. Thus, the concept is broadly concerned with social, legal, regulatory and technological measures that will ensure the integrity, confidentiality, availability and the overall security of digital information and information systems in order to achieve a high degree of trust and security necessary for the development of a sustainable information society.

This book is an attempt to discuss the legal and regulatory aspects of cybersecurity. It presents an analysis of international, regional and national regulatory responses to cybersecurity in both developed and developing countries. It highlights the limits and challenges of these regulatory responses in the promotion of cybersecurity and explores several regulatory measures to address the highlighted challenges with a view to promoting global cybersecurity. The book suggests several regulatory measures to enhance global cybersecurity and also emphasizes the need for the collective

responsibility of states for global cybersecurity. Although, developments in the criminal use of information communications technologies "continues to race ahead of the ability of regulatory frameworks to keep up", nevertheless, this book will be useful to policy makers, regulators, researchers, lawyers, students and any person interested in seeking an understanding of cybersecurity governance in developed and developing countries - especially in African countries.

This book is divided into seven chapters.
Chapter one sets out an introduction to cybersecurity law and regulation. It sets out definitions of cybersecurity and then examines the scope and basic concepts of cybersecurity as well as the critical components of cybersecurity governance. It examines a range of malicious conducts which cybersecurity laws seek to prohibit and other contextual legal issues affecting cybersecurity. The chapter then explores several "real world" perspectives to cybersecurity.

Chapter two examines several international responses and initiatives in the field of cybersecurity. It provides an analysis of the Council of Europe Convention on Cybercrime and other proposed international legal frameworks on cybersecurity such as the Commonwealth Model Law on Computer and Computer Related Crime, the Draft International Convention to Enhance Protection from Cybercrime and Terrorism, and the Global Protocol on Cybersecurity and Cybercrime. The chapter also examines the limitations of international regulatory responses on cybersecurity.

Chapter three examines the responses of some developed and technologically advanced countries as well as developing countries to cybersecurity. In this regard, the chapter basically examines legal, policy and institutional regulatory responses to cybersecurity in countries such as the United States, the United Kingdom, Singapore, India, China and Russia. It also looks at some of the major challenges that hinder cybersecurity governance in these countries.

Chapter four generally examines African multilateral regulatory responses to cybersecurity at the regional and sub-regional levels. It looks at the development of cybersecurity initiatives by the African Union and renders an analysis of the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cybersecurity in Africa. It highlights some problems of the Draft Convention and also looks at cybersecurity initiatives developed by sub-regional multilateral organizations such as the Economic Community of West African States, the Southern African Development Community and the East African Community.

Chapter five examines the national responses of African countries to cybersecurity. It provides an analysis of cybersecurity laws in several African countries that have established legal frameworks for cybersecurity such as South Africa, Botswana, Mauritius, Senegal, Kenya and Ghana. It also renders an assessment of ongoing efforts to develop legal and institutional frameworks for cybersecurity as well as other relevant cybersecurity initiatives in African countries.

Chapter six examines Nigeria's regulatory response to cybersecurity. It renders an analysis of existing and proposed regulatory frameworks on cybersecurity to determine the adequacy of these regulatory frameworks to the development of a secure and responsible information society. Nigeria is used as a case study to examine the peculiar causes of cyber-insecurity in African states as well as the peculiar challenges that hinder the effective regulation of cybersecurity in African states. The chapter also uses Nigeria as a case study to examine the implications of poor cybersecurity governance on national security, economic development, international relations, human security and human rights.

Chapter seven explores policy and regulatory strategies to enhance cybersecurity at the national, regional and global levels. It provides a summary of cybersecurity initiatives within the African region and proposes several policy and regulatory measures to enhance cybersecurity in Africa. This is then followed by proposals for policy and regulatory measures to enhance global cybersecurity. The chapter is concluded with a proposal for the collective responsibility of states for global cybersecurity. In this regard, the chapter suggests that the norm that states may be held responsible for acts and omissions within their territories which produce trans-boundary harm in other countries may also be applied for the purpose of promoting the concept of the collective responsibility of states for global cybersecurity.

This book is a modified version of a Master of Laws (LL.M) thesis originally titled: *Legal Governance of Information Technology in Nigeria and African States: An Assessment of Responses to Computer Security* which was undertaken at the Faculty of Law, University of Ibadan, Nigeria between February and April 2010 and submitted in May 2010 during the 2009/2010 academic session. However, since my graduation from the University of Ibadan in September 2010, I have taken time to modify and broaden the research to reflect some current regulatory developments in cybersecurity. I take this opportunity to express my profound gratitude to Dr. Peter Chukwuma Obutte of the Department of Public and International Law, who supervised my LL.M thesis. Dr. Obutte is one of Nigeria's leading experts in telecommunications regulation. His constructive comments and

able guidance helped in putting this work together. This made the research a cherished experience. Also his erudite guidance and tolerant disposition during our LL.M seminars is highly commendable. Following my graduation, he has also encouraged my intention to study for a Doctorate degree in Law. I would also like to express my immense gratitude to Professor Johnson O. Anifalaje for his fatherly guidance and encouragement. I am equally grateful to the Staff of the Faculty of Law Library who helped me in finding some relevant texts during the research; their devotion to duty was great.

I would also like to register my immense gratitude and appreciation to my colleagues in the LL.M Class of the 2009/2010 academic session for creating a stimulating academic environment that was favourable to intellectual growth. I would also like to thank Barr. Onyeka Kanu for his good comradeship during the short period of our study. I am very thankful to Barr. Okechukuwu Ekwanya for his assistance and good will. Barr. Okoli Pontian displayed an unwavering commitment while proof reading the manuscript and made some helpful comments of which I am very grateful.

I wish to specially thank Engr. Emmanuel Orji – a very good brother and friend, for his immense goodwill and support during my stay in Ibadan. I am equally grateful to my brother and very good friend Mr. Fredrick Onu for his sincere encouragements and goodwill. I am also grateful to my big brother Late Barr. Orji Jerome Arochukwu for his guidance and support while he was alive.

I am eternally grateful to my parents Sir & Lady Moses Orji for sponsoring my education up the Postgraduate level and also for their constant support and encouragement. I am also eternally grateful to my siblings: Engr. Ifeyinwa Orji, Dr. Ngozi Orji, Tobechukwu Orji and Ugochukwu Orji for their constant affection and support. Nothing can really describe my indebtedness to my family; hence, I am dedicating this book to them.

Uchenna Jerome Orji
Onyiba Villa,
Akanu, Amagu, Ishiagu,
Ebonyi State, Nigeria.
January 15, 2012.

Author's biography

Uchenna Jerome Orji is a Barrister and Solicitor of the Supreme Court of Nigeria. He holds a Bachelor of Laws (LL.B) honours Degree from the University of Nigeria and a Masters of Laws (LL.M) Degree with honours and distinctions from the University of Ibadan, Nigeria where he majored in Information Technology Law. Uchenna holds a national award for the best overall essay in the Fourth Edition of the Nigerian Ships and Ports Annual National Essay Competition in 2010. He is the author of *Realizing Agenda 21: A Nigerian Perspective* (Vdm Verlag: Germany, 2010) and has also been published in leading international journals including: the *Journal of International Banking Law and Regulation*, the *International Company and Commercial Law Review*, the *Computer and Telecommunications Law Review*, the *Journal of African Law*, the *Commonwealth Law Bulletin* and the *Business Law Review*. Uchenna is also an Associate and Consultant to the African Center for Cyber Law and Cybercrime Prevention (ACCP) of the United Nations, African Institute for the Prevention of Crime and the Treatment of Offenders, Kampala, Uganda (www.cybercrime-fr.org/index.pl/the_center_in_brief). He is presently undertaking Doctoral research on the regulation of telecommunications in Sub-Saharan African countries. His research seeks to explore how the regulation of telecommunications can enhance sustainable socio-economic development in Sub-Saharan Africa using Nigeria, Ghana and South Africa as case studies. The thesis involves research questions on the regulation of competition, universal access, environmental sustainability and consumer protection in the telecommunications industry. Email: jeromuch@yahoo.com.

Summary of Contents

Table of Contents

Table of Cases

United States

International Arbitration and Court Cases

Table of Legislations and Policies

AFRICAN COUNTRIES

Algeria
Cybercrime Act 2008

Angola
Basic Telecommunication Law 2001

Botswana
Cybercrime and Computer Related Crimes Act 22, 2007

Cameroon
Cybercrime Act 2011

Egypt
E-Signature Law No. 15, 2004

Ethiopia
Criminal Code of the Federal Republic of Ethiopia, Proclamation No. 414, 2004

Gambia
Information and Communications Act, No.2, 2009

Ghana
Electronic Transactions Act, No.772, 2008
National Information Technology Agency Act, No.771, 2008

Kenya
Kenyan Communications (Amendment) Act No. 1, 2009
Kenyan Information and Communications Technology Policy, 2006

Lesotho
Lesotho ICT Policy of 2005
Mauritius
Computer Misuse and Cybercrime Act No XI, 2003

Morocco
Penal Code, Law No. 07.003 of Morocco, November, 2003

Namibia
Computer Misuse and Cybercrime Act 2003

Niger
Cybercrime Law 2003

Nigeria
Advance Fee Fraud and other Fraud Related Offences Act 2006
Computer Security and Critical Information Infrastructure Protection Bill-Sb 254 2005
Constitution of the Federal Republic of Nigeria, 1999
Economic and Financial Crimes Commission (Establishment) Act 2004
Nigerian Criminal Code, Cap. 77 LFN 1990
Nigerian Communications Act 2003
National Information Technology Development Agency Act 2007
National Information Technology Policy 2001
Nigerian Cybersecurity and Data Protection Agency Bill- HB, 154 C 4443, 2008

Senegal
Senegalese Law on Cybercrime No. 2008-11 (2008)

Seychelles
Computer Misuse Act 1998
Data Protection (Amendment) Act No. 6, 2003

South Africa
South African Electronic Communications and Transactions Act No. 25, 2002
Interception and Monitoring Prohibition Act No. 127, 1992
Regulation of Interception of Communications and Provision of Communication Related Information Act (RICPCRIA) 2002
Draft Cybersecurity Policy of South Africa Government Gazette No. 32963, 19 February, 2010

Kingdom of Swaziland
Kingdom of Swaziland National Information and Communication Infrastructure (NICI) Policy 2003

Tanzania
National Information and Communications Technology Policy 2003

Tunisia
Cybercrime Act, N°1999-89, Art 199
Electronic Signature and e-commerce Law, N° 2000-83
Consumer Protection and Respect of Intellectual Property Law, N°1994-36
Data Protection Law, N°2004-63

Uganda
Computer Misuse Bill
Electronic Signature Act
E-transactions Act

Zambia
Computer Misuse and Crimes Act 2004

FOREIGN JURISDICTIONS

Brazil
Law No.9983, July 14, 2000 Article 213-13

China
Chinese Computer Information Network and Internet Security, Protection and Management Regulations 1997
Chinese Regulations on Safeguarding Computer Information Systems 1996
State Secrecy Protection Regulations for Computer Information Systems on the Internet 2000
Criminal Law of the People's Republic of China
Chinese National Defense Strategy 2010

India
Information Technology Act, No. 21, 2000
Information Technology (Amendment) Act 2008, No. 10, 2009
Information Technology (Guidelines for Cyber Cafe) Rules 2011
The Indian Cybersecurity Strategy

Mexico
Penal Code Part 9, Chapter II Article 211

Russia
Criminal Code of the Russian Federation
Law of the Russian Federation on the Legal Protection of Computer Programmes and Data Bases 1992

Russian Information Security Doctrine 2000

Singapore
Computer Misuse Act of Singapore, Cap.50A, Rev. Ed., 2007
Spam Control Act of Singapore 2007
The Infocomm Security Master Plan 2
The National Trust Framework (NTF)

United Kingdom
Anti-terrorism, Crime and Security Act 2001 (c. 24)
Computer Misuse Act 1990(c.18)
Counter-Terrorism Act 2008 (c.28)
Criminal Damage Act 1971
Extradition Act 1989
Fraud Act 2006
Police and Justice Act 2006 (c.48)
Terrorism Act 2000 (c.11)
Terrorism Act 2006 (c. 11)
Regulation of Investigatory Powers Act 2000(c.23)
The Cyber Security Strategy of the United Kingdom 2009

United States
CAN-SPAM Act 2003, Pub. L. No. 108-187, 117
Comprehensive National Cybersecurity Initiative (CNCI) 2008
Computer Fraud and Abuse Act,18 U.S.C S.1030
Cyber Security Research and Development Act, P.L. 107-305, 2002
Digital Millennium Copyright Act 1998
Economic Espionage Act, 18 U.S.C. 1832
Electronic Communications Privacy Act 1986 (ECPA) P.L. 99-508
Federal Information Security Management Act, P.L.107-347, Title III 2002
Identity Theft Restitution Act 2008
National Information Infrastructure Protection Act 1996
National Infrastructure Protection Plan 2006
National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23, January 8, 2008)
Nigerian Advance Fee Fraud Prevention Act of 1998, HR 3916 IH, 105th Congress 2d Session H. R. 3916 (Bill)
United States Cyberspace Policy Review 2009
United States National Policy on Critical Infrastructure Protection: Presidential Decision Directive No. 63, May 22, 1998
United States National Strategy to Secure Cyberspace 2003
United States International Strategy for Cyberspace 2011

United States International Cybercrime Reporting and Cooperation Bill S. 3155 and H.R. 4692 2011
United States PATRIOT Act 2001 P.L. 107-56
Wire Fraud Act 18 U.S.C Section 1343

INTERNATIONAL TREATIES, CONVENTIONS, RESOLUTIONS AND POLICY INSTRUMENTS

African Union

African Charter on Human and Peoples Rights (1981)
Constitutive Act of the African Union (2001)
Draft African Union Convention on the Establishment of a Credible Legal Framework for Cybersecurity in Africa, AU Draft0 010111, Version 01/01.2011

The Commonwealth

Model Law on Computer and Computer Related Crime LMM (02) 17

Council of Europe

Council of Europe, Convention on Cybercrime, 41 I.L.M. 282 (Budapest, 23.XI, 2001)
Additional Protocol to the Convention on Cybercrime, Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Systems, ETS No. 189
Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS No. 108 (Strasbourg, 28.I.1981)
Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse CETS No.201 (2007)

The Economic Community of West African States (ECOWAS)

ECOWAS Supplementary Act on Cybercrime and Personal Data Protection (2008)

European Union (EU)

European Convention on Human Rights (1950)
Regulation (EC) No 460/2004 establishing the European Network and information security Agency (2004)
The European Union Directive on Privacy and Electronic Communication Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (12 July, 2002)

EU Communication on a General Policy on the Fight against Cybercrime, COM (2007)
EU Data Retention Directive 2005/0182/COD
EU Communication -Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer Related Crime 26.1 2001, COM (2000)
EU Framework Decision on Attacks against Information Systems 2005/222/JHA (24 February 2005)
EU Council Framework Decision on Combating the Sexual Exploitation of Children and Child Pornography 2004/68/JHA (2003)
EU (2001) Network and Information Security- A European Policy Approach (6 June 2001)
EU Directive on Privacy and Electronic Communications (2002)

Group of Eight (G8)
G8 Okinawa Charter on Global Information Society (2000)
G8 Communiqué Annex: Principles to Combat High-Tech. Crime (1997)

Organization of American States (OAS)
OAS General Assembly Resolution AG/RES.2004 (XXXIV-o/04)
OAS General Assembly Resolution, AG/RES.2266 (XXXVII-o/07)

United Nations Conventions
United Nations Convention on the Rights of the Child (1989)
Universal Declaration of Human Rights
Optional Protocol to the Convention on the Rights of the Child on Sale of Children, Child Prostitution and Child Pornography (1989)
United Nations Convention against Transnational Organized Crime (2000)

United Nations Resolutions
Resolution 55/59 (4/12/2000)
Resolution 60/177 (16/12/2005)
Rio Declaration on the Environment and Development (1992)
Stockholm Declaration (1972)

United Nations Resolutions on Combating the Criminal Misuse of Information Technology
Resolution 55/63 (A/RES/55/63) of 4 December 2000
Resolution 56/121 (A/RES/56/121) of 19 December 2001

United Nations Resolutions on the Creation of a Global Culture of Cybersecurity

Resolution 57/23 (A/RES/57/239) 20 December 2002
Resolution 58/199 on the Creation of a Global Culture of Cybersecurity and Protection of Critical Information Infrastructures (A/RES 58/199) 23 December 2003

United Nations Resolutions on Developments in the Field of Telecommunications in the Context of International Security

Resolution 55/28 (20/11/2000)
Resolution 56/164 (A/56/164)
Resolutions 53/70 (4/12/1998)
Resolution 55/28 (28/11/20000
Resolution 54/49 (12/1999)
Resolution 56/19 (29/11/2001)
Resolution 58/32 (18/12/2003)
Resolution 59/61 (3/12/2004)
Resolution 60/45 (8/12/2005)
Resolution 61/54 (6/12/2006)
Resolution 62/17 (5/12/2007)
Resolution 63/37 (2/12/2008)

United Nations Economic and Social Council (ECOSOC) Resolutions

(ECOSOC) Resolution 2002/10
ECOSOC Resolution 2004/26
ECOSOC Resolution 2007/20 (26/7/2007)
ECOSOC Resolution 2004/42
ECOSOC Resolution 2009/22 (30/7/2009)

Resolutions of the United Nations Commission on Narcotic Drugs

Resolution 48/5 on Strengthening International Cooperation in Order to Prevent the Use of the Internet to Commit Drug Related Crime

Subsidiary Legal and Policy Instruments

Draft Code on Peace and Security in Cyberspace - A Global Protocol on Cybersecurity and Cybercrime
Draft International Convention to Enhance Protection from Cybercrime and Terrorism
OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (25 July 2002)
Resolution 52 – Countering and Combating Spam (WTSA-08 –

Resolution 52) World Telecommunication Standardization Assembly Johannesburg, (21-30 October 2008)
World Summit on the Information Society (WSIS) *Declaration of Principles, Building the Information Society: A Global challenge in the New Millennium* (2003)
World Summit on the Information Society (WSIS) *Plan of Action* (2003)
World Summit on the Information Society (WSIS) *The Tunis Agenda for the Information Society* (2005)

List of Tables and Figures