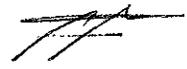


SENATE
S. No. **3327**



Introduced by Senator Miriam Defensor Santiago

EXPLANATORY NOTE

The use of information and communications technology (ICT) and of the Internet has brought about a sea of change in the lives of ordinary Filipinos. Rare now are the queues before public pay telephones; today, the penetration of mobile phone subscription is pegged by the World Bank at 92%.¹ Uncommon today are the handwritten letters and voice tapes exchanged between OFWs and their families and friends; instead, families communicate in real time or in near-real time via Skype, Facebook, Chikka internet-based texting, and email. Students and academics are no longer limited by the size and comprehensiveness of the local library; today, even advanced studies done in developed countries are available to the furthest rural classroom that is equipped with a computer and a broadband connection.²

ICT has likewise been a boon to the Philippine economy. According to a 2009 World Bank study of ICT's impact on economies, for every ten percentage-point increase in high-speed Internet connections there is an increase in economic growth of 1.3 percentage points—contrast this with 0.8 percentage point increase in economic growth per ten percentage point increase in mobile phone subscriptions.³ Through fast and reliable corporate networks, the BPO, ITO, and other outsourcing industries have contributed USD 11 billion in export revenues, contributing an

¹ Data from World Development Indicators (WDI, or World dataBank <http://databank.worldbank.org/>); the primary World Bank database for development data from officially-recognized international sources.

² "Skype brings OFW families together at Noche Buena", GMA News Online, 29 December 2011 (<http://www.gmanetwork.com/news/story/243034/scitech/socialmedia/skype-brings-ofw-families-together-at-noche-buena>); "More Filipinos now using Internet for news, information – study", GMA News Online, 31 January 2012 (<http://technology.inquirer.net/8013/more-filipinos-now-using-internet-for-news-information-study>)

³ "Information and Communications for Development 2009: Extending Reach and Increasing Impact", World Bank, 22 July 2009 (permanent URL: <http://go.worldbank.org/NATLOH7HV0>; online reading: <http://issuu.com/world.bank.publications/docs/9780821376058>)

estimated 5.4% to the country's GDP in 2011.⁴ The salary scales of the average knowledge worker ranged from PHP 10,000 to PHP 100,000 in 2006,⁵ lessening the pressure for college graduates and professionals to seek employment abroad.⁶

Many government officials and agencies have learned that ICT and the Internet have been powerful tools to promote their agendas and engage the citizenry. As early as 2006, former councilor Peter Laviña had advocated C2G/G2C (citizen to government/ government to citizen) participative governance in Davao City through his eponymous former governance blog "Peter Laviña",⁷ and various officials have now adapted this practice via their personal blogs, Facebook fan pages, and Twitter accounts. ICT tools and the Internet proved invaluable in disaster management, rescue and relief operations during Ondoy, Pepeng, and Habagat;⁸ today, communication through the Internet and social media are the hallmark of the well-loved public service of PAGASA (@dost_pagasa), Project Noah (<http://noah.dost.gov.ph/>), and the MMDA (@mmda). The use of ICT, the Internet, and social media can even be argued to have been key to the election of President Benigno "Noynoy" Aquino III.⁹

But even as the Philippines learned to harness ICT and the Internet for the good, the dark side of ICT and Internet use has not been a stranger to our shores. This has not escaped the notice of our legislators. Shortly after the Internet was first used in the country in 1994,¹⁰ and over the years since, legislators have crafted measures to ensure the protection of the public, such as the Electronic Commerce Act (R.A. No. 8792), the Data Privacy Act (R.A. No. 10173). Unfortunately, there remains legislation that confine the Philippines to 20th century capabilities

⁴ "After dominating call centers, Philippine IT-BPO seeks world leadership in four more fast growing services", DOST-ICTO, 30 January 2012 (http://www.dost.gov.ph/index.php?option=com_content&view=article&id=1096)

⁵ "An Input-Output Analysis of the Philippine BPO Industry", Magtibay-Ramos, Estrada, Felipe, 2 October 2007 (<http://www.nscb.gov.ph/ncs/10thNCS/papers/invited%20papers/ips-02/ips02-03.pdf>)

⁶ "BPO industry expects more dramatic growth ahead", The Manila Times, August 5, 2012 (<http://www.manilatimes.net/index.php/sunday-times/front-pages/28372-bpo-industry-expects-more-dramatic-growth-ahead>); "BPO Sector Can Surpass OFW Remittances With Gov't Support - Angara", Senator Edgardo Angara, 8 June 2011 (http://www.senate.gov.ph/press_release/2011/0608_angara2.asp)

⁷ "The ABCs of Councilor Laviña", Peter Laviña, March 9, 2006 (<http://peterlavina.blogspot.com/2006/03/abcs-of-councilor-lavia.html>)

⁸ "ANC interview with Communications Undersecretary Manuel L. Quezon III, on engagement through new media platforms", Presidential Communications Development & Strategic Planning Office, 14 August 2012 (<http://pcdsp.gov.ph/2012/08/14/anc-interview-with-communications-undersecretary-manuel-l-quezon-iii-on-engagement-through-new-media-platforms/>)

⁹ "Facebook and Twitter — democratising participation in the Philippines", Social Media and Politics: Online Social networking and Political Communication in Asia, Espina-Letargo, 2010 (http://www.kas.de/wf/doc/kas_21591-1522-1-30.pdf?110120093225)

¹⁰ "Developing a Viable Framework for Commercial Internet Operations in the Asia-Pacific Region: The Philippine Experience", Paraz, 1997 (http://www.isoc.org/inet97/proceedings/E6/E6_1.HTM)

in this 21st century information society, for instance, the Public Telecommunications Policy Act of 1995 (R.A. No. 7925) must be updated to deal with 21st century issues. Clearly, laws that have an impact on cyberspace must address the realities of the present and the challenges of the future: The strands of law enforcement and economic development, among others, harmonized into a unified framework responsive to the needs of the public and of government.

Furthermore, international and transnational threats to the national security of the Philippines through the use of ICT and the Internet are made known on a daily basis. With each institution that falls prey to the designs of cyber terrorists, new vulnerabilities of Philippine institutions are likewise discovered. Various international treaties, agreements, and conventions, such as the UN Convention Against Transnational Organized Crime, the International Convention for the Suppression of the Financing of Terrorism, and the Budapest Convention have highlighted the need for nation-states to secure their ICT and Internet infrastructure. Reports on the use of ICT as weapons, such as the alleged deployment of the “Stuxnet” worm by the United States against Iran,¹¹ and the alleged hacking of the People’s Republic of China of Google servers,¹² and the recent attack on Middle Eastern oil production infrastructure by the Shamoon virus,¹³ have shown the world that ICT can be used as weapons, and thus impressed upon the world’s leaders to develop their own countries’ cybersecurity and cyberdefense capabilities.

The Magna Carta for Philippine Internet Freedom is envisioned to ensure that the Philippines and its individual citizens are able to meet the challenges posed by ICT and cyberspace, able to wield it and benefit from it in charting a better future. The urgency of this legislation cannot be gainsaid, and we trust that the legislators will see the wisdom of this law.

ocr

MIRIAM DEFENSOR SANTIAGO

¹¹ "Obama Order Sped Up Wave of Cyberattacks Against Iran", New York Times, Sanger, 1 June 2012 (<http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html>)

¹² "Top Chinese officials ordered attack on Google, Wikileaks cables claim", The Telegraph, Sawyer, 4 December 2010 (<http://www.telegraph.co.uk/news/worldnews/wikileaks/8181619/Top-Chinese-officials-ordered-attack-on-Google-Wikileaks-cables-claim.html>)

¹³ "'Shamoon' virus most destructive yet for private sector, Panetta says", Chicago Tribune, Stewart, 11 October 2012 (<http://www.chicagotribune.com/news/sns-rt-us-usa-cyber-pentagon-shimoonbre89b04y-20121011.0.5793512.story>)

Table of Contents

	Page
The Magna Carta for Philippine Internet Freedom	1
Part 1. Preliminary Provisions	1
Chapter I. General Provisions	1
Section 1. Title	1
Section 2. Declaration of Policy	1
Chapter II. Definition of Terms	3
Section 3. Definitions	3
Part 2. Internet Rights and Freedoms	12
Chapter III. Internet Rights and Freedoms	12
Section 4. Protection of the Internet as an open network	12
Section 5. Promotion of network neutrality	12
Section 6. Promotion of universal access to the Internet	12
Section 7. Right to privileged access to devices	14
Section 8. Right to freedom of speech and expression on the Internet	14
Section 9. Protection of the freedom to innovate and create without permission	15
Section 10. Right to privacy of data	16
Section 11. Right to security of data	16
Section 12. Protection of intellectual property	18
Section 13. Promotion of development of Internet, network, and information and communications infrastructure	19
Chapter IV. Compliance With Treaty Obligations and International Conventions	19
Section 14. Declaration of Compliance	19
Chapter V. Duties Related the Promotion of Internet Freedom	20
Section 15. The State as the Primary Duty Bearer	20
Section 16. Duties of the State Agencies and Instrumentalities	20
Chapter VI. Regulations for the Promotion of Internet Freedom	25
Section 17. Amendments to the Public Telecommunications Policy Act of the Philippines	25
Section 18. Quality of Service and Network Fair Use	36
Section 19. Amendments to the Intellectual Property Code of the Philippines	38
Section 20. Content Fair Use	43
Section 21. Amendments to the e-Commerce Act	44
Section 22. Amendments to the Data Privacy Act	44
Section 23. Repeal of the Anti-Cybercrime Law	44
Part 3. Cybercrime	45
Chapter VII. Cybercrimes and Other Prohibited Acts	45
Section 24. Network sabotage	45
Section 25. Failure to Provide Reasonable Security for Data and Networks	45

Section 26. Violation of Data Privacy	46
Section 27. Violation of Data Security	47
Section 28. Illegal and Arbitrary Seizure	49
Section 29. Infringement of Intellectual Property Rights	50
Section 30. Fraud via ICT	51
Section 31. ICT-Enabled Prostitution and ICT-Enabled Trafficking in Persons	51
Section 32. ICT-Enabled Child Prostitution and ICT- Enabled Child Trafficking	53
Section 33. Internet Libel, Hate Speech, Child Pornography, and Other Expression Inimical to the Public Interest	56
Section 34. Sabotage of critical networks and infrastructure, and other acts of cyberterrorism	59
Chapter VIII. Penalties	62
Section 35. Applicability of the Revised Penal Code.	62
Section 36. Penalties For Specific Violations of The Magna Carta for Philippine Internet Freedom.	62
Section 37. Penalties for Violations of the Magna Carta for Philippine Internet Freedom Affecting Critical Networks and Infrastructure.	70
Section 38. Penalties for Other Violations of The Magna Carta for Philippine Internet Freedom.	70
Section 39. Penalties for Violations of The Magna Carta for Philippine Internet Freedom Committed by a Public Official or Employee.	70
Section 40. Liability Under the Data Privacy Act, the Intellectual Property Code, the Optical Media Act, the Anti-Child Pornography Act of 2009, the Revised Penal Code, and Other Laws.	71
Chapter IX. Cybercrime Law Enforcement and Jurisdiction	72
Section 41. Competent Law Enforcement Agencies	72
Section 42. Cybercrime Courts	72
Section 43. Jurisdiction of Cybercrime Courts	73
Section 44. Extraterritorial Application of the Magna Carta for Philippine Internet Freedom	74
Part 4. Cyberdefense and National Cybersecurity	75
Chapter X. National Cybersecurity and Cyberdefense	75
Section 45. Cyberwarfare and National Defense.	75
Section 46. National Cybersecurity and Protection of Government Information and Communications Technology Infrastructure.	75
Section 47. Amendments to the AFP Modernization Act.	76
Chapter XI. Counter-Cyberterrorism	78
Section 48. Counter-Cyberterrorism.	78
Part 5. Final Provisions	79
Chapter XII. Implementing Rules and Regulations	79

Section 49. General Implementing Rules and Regulations for the Implementation of the Magna Carta for Philippine Internet Freedom.	79
Section 50. Implementing Rules and Regulations for Information and Communications Technology Infrastructure Development.	79
Section 51. Implementing Rules and Regulations for Cybercrime Law Enforcement.	80
Section 52. Implementing Rules and Regulations for Information and Communications Technology Education, Training, and Human Resources.	80
Section 53. Implementing Rules and Regulations for Information and Communications Technology Research and Development.	81
Section 54. Implementing Rules and Regulations for National Cyberdefense, Cyberintelligence, and Counter-Cyberterrorism.	81
Section 55. Implementing Rules and Regulations for Government Information and Communications Infrastructure and National Cybersecurity.	83
Chapter XIII. Periodic Review Clause	84
Section 56. Periodic Review of the Implementing Rules and Regulations of the Magna Carta for Philippine Internet Freedom.	84
Chapter XIV. Transitory Provisions	84
Section 57. Appointment of the Secretary of Information and Communications Technology.	84
Section 58. Release of Initial Appropriations.	84
Section 59. Preparation of Implementing Rules and Regulations.	84
Section 60. Compliance of Government ICT Infrastructure and Critical Networks, Data, and Internet Infrastructure.	85
Chapter XV. Public Information Campaign	85
Section 61. Public Information Campaign for the Magna Carta for Philippine Internet Freedom and its Implementing Rules and Regulations.	85
Chapter XVI. Appropriations	86
Section 62. Initial funding requirements.	86
Section 63. Succeeding appropriations.	87
Chapter XVII. Separability Clause	87
Section 64. Separability clause.	87
Chapter XVIII. Repealing Clause	87
Section 65. Repealing clause.	87
Chapter XIX. Effectivity Clause	87
Section 66. Effectivity clause.	87

SENATE
S. No. 3327



Introduced by Senator Miriam Defensor Santiago

1 AN ACT
2 ESTABLISHING A MAGNA CARTA FOR PHILIPPINE INTERNET FREEDOM,
3 CYBERCRIME PREVENTION AND LAW ENFORCEMENT, CYBERDEFENSE
4 AND NATIONAL CYBERSECURITY

Be it enacted by the Senate and House of Representatives of the Philippines in Congress assembled:

5 **Part 1. Preliminary Provisions**

6 **Chapter I. General Provisions.**

7 *Section 1. Short Title.* – This Act shall be known as “The Magna Carta for Philippine
8 Internet Freedom.”

9 *Section 2. Declaration of Policy.* –

10 1. The State reaffirms its recognition of the vital role of communication and information
11 in nation-building, as stated in Article II, Section 24, of the Constitution.

12 2. The State affirms that all the rights, guarantees, and privileges provided by the 1987
13 Constitution, especially the rights guaranteed by Article III, and the rights, guarantees and
14 privileges provided by treaties and conventions to which the Philippines is a signatory and
15 general principles of international law, shall apply to the Filipino people in their use,
16 development, innovation, and invention of information and communications technology (ICT)
17 and the Internet.

18 3. The State affirms its commitment to the people and to all nations that, in the crafting of
19 laws and regulations governing the use of the Internet and of information and communications
20 technology, these shall be subject to Article I, II, III, and IV of the Constitution.

1 4. Recognizing that art, beauty, and culture can be created on devices, on networks, and
2 on the Internet, the State shall pursue a policy that promotes the Internet and information and
3 communications technology, and the innovation therein and thereof, as instruments of life,
4 liberty, and the pursuit of happiness.

5 5. Recognizing that the growth of the Internet and information and communications
6 technologies both depend on and contribute to the growth of the economy, advances in science
7 and technology, and the development of human capital, and encourage democratic discourse and
8 nation-building, the State reaffirms its commitments to education, to science and technology, to
9 labor, and to private enterprise. Further, the State recognizes that development, invention, and
10 innovation for the Internet and for information and communications technology are pursuits of
11 both the public and the private sector, and can be local, national, international, and transnational
12 in effort. Therefore, the State shall endeavor to develop plans, policies, programs, measures, and
13 mechanisms to encourage development, invention, and innovation through and for the Internet
14 and for information and communications technology, in cooperation with other nations and
15 international bodies.

16 6. Recognizing that the growth of the Internet and information and communications
17 technologies affect peace and order and the enforcement of law within the national territory and
18 *across other nations, the State reaffirms its policy of cooperation and amity with all nations, and*
19 *its adoption of generally accepted principles of international law as part of the law of the land, in*
20 *the pursuit of peace and order and in the enforcement of law.*

21 7. Recognizing that the Internet has the potential to become a theater of war, and that
22 information and communications technologies can be developed into weapons of mass
23 destruction, the State reaffirms its renunciation of war as an instrument of national policy.
24 Therefore, consistent with the national interest, the State shall pursue a policy of “no first use” of
25 cyberweapons against foreign nations and shall pursue a policy of cyberdefense, and shall
26 endeavor to develop plans, policies, programs, measures, and mechanisms to provide security for
27 Internet and information and communications technology infrastructure for and in the defense of
28 the Filipino people.

29

1 2. Administrator – A person or role with privileged access and control over a network or
2 a multi-user computing environment responsible for the operation and the maintenance of the
3 network or computing environment.

4 2.1. Network administrator – A person or role responsible for the operation and
5 the maintenance of a network.

6 2.2. Systems administrator – A person or role responsible for managing a multi-
7 user computing environment.

8 3. Availability – The ability of a device or set of devices to be in a state to perform a
9 required function under given conditions at a given instant of time or over a given time interval,
10 assuming that the required external resources are provided.

11 4. Bandwidth – The capacity of a transmission medium to carry data.

12 5. Bot – A computer program or software installed in a device, computer, computer
13 system, or network capable of performing automated tasks over the Internet, without the
14 knowledge or consent of the user or owner of the device computer, system, or network, with
15 control ceded to a third party, usually malicious. Bot may also refer to the individual device that
16 is infected with such programs or software.

17 5.1. Botnet – A network of computers infected with bots.

18 6. Cache – A temporary storage of recently accessed data or information, which may be
19 stored in the local storage medium of a device or computer, or in the storage media of a network,
20 for purposes of speeding up subsequent retrievals of data or information from the Internet or
21 networks.

22 7. Code – The symbolic arrangement of data or instructions in a computer program or a
23 set of such instructions.

24 8. Component – Any individual part of a device.

25 9. Computer – Any device or apparatus which, by electronic, electro-mechanical or
26 magnetic impulse, or by other means, is capable of receiving, recording, transmitting, storing,
27 processing, retrieving, or producing information, data, figures, symbols or other modes of written
28 expression according to mathematical and logical rules or of performing any one or more of
29 those functions.

1 10. Computer program – A set of instructions expressed in words, codes, schemes or in
2 any other form, which is capable when incorporated in a medium that the computer can read, of
3 causing the computer to perform or achieve a particular task or result.

4 11. Configuration – The way a device, computer, computer system, or network is set up.

5 12. Content – Data that can be readily understood by a user immediately upon access,
6 which may include but is not limited to text, pictures, video, or any combination thereof. The
7 word is synonymous to information. Data that is readable and usable only by and between
8 devices, computers, systems or networks, such as traffic data, is not content.

9 13. Control – The use of resources, modification of the configuration, and otherwise
10 exertion of a directing influence on the operation of a device, computer, system, or network.

11 14. Critical infrastructure – The systems and assets, whether physical or virtual, so vital
12 to the Philippines that the incapacity or destruction of such systems and assets would have a
13 debilitating impact on national security, economy, public health or safety, or any combination of
14 those matters.

15 15. Critical network – An information and communications system or network of
16 systems, whether physical or virtual, so vital to the Philippines that the incapacity or destruction
17 of such a network would have a debilitating impact on national security, economy, public health
18 or safety, or any combination of those matters.

19 16. Cryptography – The discipline which embodies principles, means, and methods for
20 the transformation of data in order to hide its information content, prevent its undetected
21 modification and/or prevent its unauthorized use. (

22 17. Cyber environment – The environment comprised of users, networks, devices, all
23 software, processes, information in storage or transit, applications, services, and systems that can
24 be connected directly or indirectly to networks or the Internet.

25 18. Cyberattack – An attack by a hostile foreign nation-state or violent non-state actors
26 on Philippine critical infrastructure or networks through or using the Internet or information and
27 communications technology. The term may also be used to mean an assault on system security
28 that derives from an intelligent threat, *i.e.*, an intelligent act that is a deliberate attempt to evade
29 security services and violate the security policy of a system.

1 19. Cybercrime – Any unlawful act punishable by this law or other relevant laws
2 committed through or using the Internet or information and communications technology.

3 20. Cyberdefense – The collection of plans, policies, programs, measures, mechanisms,
4 and weapons designed to defend the Philippines from cyberattack.

5 21. Cyberintelligence – The collection, analysis, processing, and dissemination of
6 information, which may be done through or using the Internet or information and
7 communications technology, designed to provide guidance and direction to commanders and
8 leaders of military and law enforcement units towards the combating of acts of cyberattack and
9 cyberterrorism.

10 22. Cybersecurity – The collection of tools, policies, security concepts, security
11 safeguards, guidelines, risk management approaches, actions, training, best practices, assurance,
12 and technologies that can be used to protect the cyber environment and organization and user's
13 information and communications technology assets.

14 23. Cyberspace – A global domain within the information environment consisting of the
15 interdependent network of information systems infrastructures including the Internet,
16 telecommunications networks, computer systems, and embedded processors and controllers, or
17 the virtual space constituted by a computer network with a set of distributed applications and its
18 users.

19 24. Cyberterrorism – A violation of the Human Security Act of 2007 committed through
20 or using the Internet or information and communications technology.

21 25. Cyberwarfare – The actions by a nation-state or international organization to attack
22 and attempt to cause damage to another nation through or using computers, information and
23 communications technology, networks, or the Internet.

24 26. Data – The reinterpretable representation of information in a formalized manner
25 suitable for communication, interpretation, or processing, or information represented in a manner
26 suitable for automatic processing.

27 26.1. Data, private – Any and all data that does not fall under the definition of public
28 data.

1 26.2. Data, public – Data which is available to the public without access being restricted
2 by requirements of membership, non-disclosure agreements or similar.

3 27. Device – The material element or assembly of such elements intended to perform a
4 required function.

5 28. Download – The transfer of data or information from the Internet or a network to a
6 device or computer upon request of the user for this information.

7 29. Encryption – An encoding scheme that produces meaningless information to all
8 observers except those with the decoding key.

9 30. End user license agreement – The legal agreement between two parties, one of which
10 is the user, that stipulates the terms of usage of a device, software, or service.

11 31. Equipment – A single apparatus or set of devices or apparatuses, or the set of main
12 devices of an installation, or all devices necessary to perform a specific task.

13 31.1. Data processing equipment – Equipment used to process data.

14 31.2. Network equipment – Equipment used to allow data communication between
15 devices, computers, systems, networks, or the Internet.

16 31.3. Storage equipment – Equipment used to store data.

17 32. Executable – The ability of a code, script, software, or computer program to be run
18 from start to finish in a device or computer, and providing a desired result.

19 33. Free and open-source software – Liberally licensed software whose license grants
20 users the right to use, copy, study, change, and improve its design through the availability of its
21 source code.

22 34. Hardened – The state of reduced vulnerability to unauthorized access or control or to
23 malicious attacks of a device, computer, network, or information and communications
24 technology infrastructure.

25 35. Hardware – The collection of physical elements that comprise a device, equipment,
26 computer, system, or network.

27 36. High-speed connection – A service that provides data connection to networks and the
28 Internet that has data rates faster than what is generally available to the general public.

1 37. High-volume connection – A service that provides data connection to the networks
2 and the Internet that allows volumes of uploadable and/or downloadable data larger than what is
3 generally available to the general public.

4 38. Information – Data that can be readily understood by a user immediately upon access,
5 which may include but is not limited to text, pictures, video, or any combination thereof. The
6 word is synonymous to content. Data that is readable and usable only by and between devices,
7 computers, systems or networks, such as traffic data, is not information.

8 38.1. Private information – Refers to any of these three classes of information: (1)
9 any information whether recorded in a material form or not, from which the identity of an
10 individual is apparent or can be reasonably and directly ascertained by the entity holding
11 the information, or when put together with other information would directly and certainly
12 identify an individual; (2) Any and all forms of data which under the Rules of Court and
13 other pertinent laws constitute privileged communication; and, (3) any information whose
14 access requires the grant of privileges by a duly-constituted authority, which may include
15 but is not limited to a systems or network administrator.

16 38.2. Sensitive private information – Refers to personal information: (1) About an
17 individual's race, ethnic origin, marital status, age, color, and religious, philosophical or
18 political affiliations; (2) About an individual's health, education, genetic or sexual life of
19 a person, or to any proceeding for any offense committed or alleged to have been
20 committed by such person, the disposal of such proceedings, or the sentence of any court
21 in such proceedings; (3) Issued by government agencies peculiar to an individual which
22 includes, but not limited to, social security numbers, previous or current health records,
23 licenses or its denials, suspension or revocation, and tax returns; and (4) Specifically
24 established by an executive order or an act of Congress to be kept classified.

25 38.3. Public information – Any information that is not restricted by virtue of the
26 preceding definitions and can be readily accessed by any interested member of the public.

27 39. Information and communications technology – The integration of real-time
28 communication services, non-real-time communication services, and telecommunications,

1 computers, software, hardware, storage, and devices, which enable users to access, store,
2 transmit, and manipulate information.

3 40. Internet – The global system of interconnected computer networks linked by various
4 telecommunications technologies and that uses the standard Internet protocol suite.

5 41. Medium – A material used for specific purposes.

6 41.1. Storage medium – The physical material or device in which data or
7 information may be stored, which includes but is not limited to magnetic tape, disk
8 drives, flash devices, electrically erasable programmable read-only memory (EEPROM)
9 chips, optical media disks, punched cards, and paper.

10 41.2. Transmission medium – The physical material through which a data
11 communication signal is transmitted, which includes but is not limited to twisted-pair
12 copper wire, coaxial cable, optical fiber, and air.

13 42. Network – A collection of computers, devices, equipment, and other hardware
14 interconnected by communication channels that allow sharing of resources and information.

15 42.1. Private network – A network which is operationally private by nature and
16 not universally accessible by the general public.

17 42.2. Public network - A network which provides services to the general public.

18 43. Offline – The state of being disconnected from the Internet or networks.

19 44. Online – The state of being connected to the Internet or a network.

20 45. Ownership – Ownership is defined by the Civil Code.

21 45.1. Privately-owned – Ownership as provided for by the Civil Code of the
22 Philippines by a natural person or a juridical person under Article 44 paragraph (3) of the
23 Civil Code.

24 45.2. Publicly-owned – Ownership as provided for by the Civil Code of the
25 Philippines by a juridical person under Article 44 paragraphs (1) and (2) of the Civil
26 Code.

27 46. Physical plant – The building, structure, and infrastructure necessary to support and
28 maintain a facility.

1 47. Privacy – May refer to any of these definitions, or a combination of these definitions:
2 (1) the right guaranteed and protected by the Constitution; (2) the right of individuals to control
3 or influence what personal information related to them may be collected, managed, retained,
4 accessed, and used or distributed; (3) the protection of personally identifiable information; and,
5 (4) a way to ensure that information is not disclosed to anyone other than the intended parties
6 (also known as "confidentiality").

7 48. Privilege – A right that, when granted to an entity, permits the entity to perform an
8 action.

9 48.1. Privileged access – The completely unrestricted access of a user to the
10 resources of a device, computer, system, or network.

11 48.2. Privileged control – The completely unrestricted ability of a user to use the
12 resources, modify the configuration, and otherwise exert a directing influence on the
13 operation of a device, computer, system, or network.

14 49. Processing – The act of performing functions or activities on data or information.

15 49.1. Processing (Data Privacy Act) – Any operation or any set of operations
16 performed upon personal information including, but not limited to, the collection,
17 recording, organization, storage, updating or modification, retrieval, consultation, use,
18 consolidation, blocking, erasure or destruction of data. (RA 10173)

19 49.2. Data processing – Any process to enter data and summarize, analyze or
20 otherwise convert data into usable information.

21 49.3. Information processing – The transformation of information in one form to
22 information in another form through an algorithmic process.

23 50. Protocol – A defined set of procedures adopted to ensure communication, or a set of
24 rules for data transmission in a system interlinking several participants.

25 51. Publication – the act of making works available to the public by wire or wireless
26 means in such a way that interested members of the public may access these works from a place
27 and time individually chosen by them.

28 52. Script – A computer program or sequence of instructions that is interpreted or carried
29 out by another computer program instead of directly by a computer, device, or equipment.

1 53. Security – The ability to prevent fraud as well as the protection of information
2 availability, integrity and confidentiality.

3 53.1. Security by behavioral means – The use of laws, regulations, policies,
4 procedures, instructions and the like to influence or restrict behavior for purposes of
5 maintaining security.

6 53.2. Security by electronic means – The use of computer programs, software,
7 code, scripts, devices, or equipment for purposes of maintaining security.

8 53.3. Security by physical means – The use of locks, gates, security guards and
9 other analogous means, for purposes of maintaining security.

10 54. Service – A set of functions offered to a user by another person or by an organization.

11 54.1. Service quality – The collective effect of service performance which
12 determines the degree of satisfaction of a user of the service.

13 55. Software – The set of programs, procedures, algorithms and its documentation
14 concerned with the operation of a data processing system, computer, device, or equipment.

15 55.1. Software application – Software designed to help a user perform a specific
16 task or set of tasks.

17 56. Telecommunications – A service or system of interconnected entities providing the
18 ability to exchange and interchange data between points or from a point to multiple points.

19 57. Upload – The transfer of data or information to the Internet or a network from a
20 device or computer, initiated by the user.

21 58. Uptime – The time a device, equipment, computer, or network can be left unattended
22 without suffering failure, or needing to be undergo administrative or maintenance purposes.

23 59. User – Any person, whether natural or juridical, or any entity that makes use of a part
24 or whole of the resources of a device, equipment, computer, system, network, software, software
25 application, code, or script.

26 60. Virus – Any computer program, code, or script that implements unauthorized and/or
27 undesirable changes to a device, computer, equipment, system, or network. For purposes of this
28 Act, the term may be used synonymously with malware, spyware, worms, trojans, and the like.

1 **Part 2. Internet Rights and Freedoms**

2 **Chapter III. Internet Rights and Freedoms**

3 *Section 4. Protection of the Internet as an open network. –*

4 1. The State shall, within its jurisdiction, protect and promote the Internet as an open
5 network.

6 2. Except for customer premises equipment as defined by this Act and other relevant
7 laws, no person shall restrict or deny the interconnection or interoperability of a device, an
8 equipment, or a network that is capable of such interconnection or interoperability to the Internet,
9 to other public networks, or to other Internet service providers, telecommunications entities, or
10 other such persons providing Internet or data services, without due process of law or authority
11 vested by law. The interoperability of a device, an equipment, or a network within a private
12 network may be restricted by the duly authorized system and/or network administrators of the
13 private network, subject to the provisions of the Data Privacy Act and other relevant laws.

14 *Section 5. Promotion of network neutrality. –* No person shall restrict the flow of data or
15 information on the Internet on the basis of content, nor shall any person institute and employ
16 means or methods to favor the flow of information on the Internet of one class of data or
17 information over another on the basis of content, except: a) if the data or information whose flow
18 is being favored is used to solely to manage the security or service quality of a network, or of an
19 Internet or data service, and; b) the data or information whose flow is being favored cannot be
20 used for any other purpose other than the management of security or service quality of the
21 network.

22 *Section 6. Promotion of universal access to the Internet. –*

23 1. The State shall, within its jurisdiction, protect and promote universal access to the
24 Internet.

25 2. No person shall restrict or deny another person access to the Internet without an Order
26 issued by a court of competent jurisdiction, issued after notice and hearing, showing probable
27 cause that the person's access to the Internet is a means for the commission of:

1 (a) the felonies of Robo, Hurto, Estafa, Falsification, and Malversation, as defined
2 in the Revised Penal Code;

3 (b) any criminal offense defined and punishable in the following special penal
4 laws: the Anti-Trafficking in Persons Act of 2003, the Anti-Graft and Corrupt Practices
5 Act, the Code of Conduct and Ethical Standards for Public Officials and Employees, the
6 Anti-Money Laundering Act of 2001, the Violence Against Women and Children Act,
7 the Special Protection of Children Against Abuse, Exploitation, and Discrimination Act,
8 the Child and Youth Welfare Code, the Anti-Child Pornography Act of 2009, the Human
9 Security Act of 2007, or the Data Privacy Act of 2012; or

10 (c) any criminal offense defined and punishable by this Act.

11 3. Except in cases where the Petition specifies that the Internet is used to commit an act
12 that is defined and penalized by the Violence Against Women and Children Act or the Anti-
13 Child Pornography Act of 2009, no Order shall be issued restricting access to the Internet for
14 more than sixty (60) days, or until the preliminary investigation for the predicate offense shall
15 have concluded, whichever is shorter.

16 4. Should an Information be filed on any one of the predicate offenses mentioned in this
17 section, the Order restricting access to the Internet shall continue until the trial on the merits has
18 terminated.

19 5. Should the accused be convicted of the predicate offense, the Order restricting access
20 to the Internet shall continue until the person's criminal liability is extinguished.

21 6. No natural or juridical person, offering Internet access or by whose nature there is a
22 reasonable expectation of Internet access, including but not limited to any hotel, restaurant,
23 school, religious group, organization, or association, shall restrict access to the Internet or any
24 other public communications network from within its private network, or limit the content that
25 may be accessed by its employees, students, members, or guests, without a reasonable ground
26 related to the protection of the natural or juridical person from actual or legal threats, the privacy
27 of others who may be accessing the network, or the privacy of information in the network as
28 provided for in the Republic Act No. 10173 aka the "Data Privacy Act of 2012."

1 *Section 7. Right to privileged access to devices. –*

2 1. The State shall, within its jurisdiction, protect the right of a person to gain or attain
3 privileged access or control over any device over which the person has property rights.

4 2. It shall not be unlawful for any person involved in the wholesale or retail of devices to
5 install, implant, or otherwise put in a device a component, a configuration, or code that shall
6 restrict the operation of a device; Provided, the installation or implantation is for the sole purpose
7 of ensuring the privacy or security of the interconnection or interoperability of the device with
8 public or private networks or Internet or information and communications technology
9 infrastructure.

10 3. Subject to the law on contracts and other relevant laws on product warranty and
11 consumer welfare, it shall not be unlawful for any person who, by physical, electronic, or any
12 other means, shall gain or attain privileged access or control over any device over which the
13 person has property rights; Provided, the gain or attainment of privileged access or control was
14 not intended to circumvent the protection of or cause the actual infringement on intellectual
15 property rights of another person.

16 *Section 8. Right to freedom of speech and expression on the Internet. –*

17 1. The State shall, within its jurisdiction, protect and promote the freedom of speech and
18 expression on the Internet.

19 2. The State shall, within its jurisdiction, protect the right of the people to petition the
20 government via the Internet for redress of grievances.

21 3. The State shall, within its jurisdiction, protect the right of any person to publish
22 material on or upload information to the Internet.

23 4. No person shall be compelled to restrict access to information on the Internet or to
24 remove published material or uploaded information from the Internet except upon Order
25 following a special proceeding for the purpose before a Regional Trial Court of competent
26 jurisdiction, upon a determination by the Court that:

27 (a) the nature of the material or information creates a clear and present danger of a
28 substantive evil that the state has a right or duty to prevent;

1 (b) the material or information is not protected expression under the standards of
2 the community or the audience toward which the material or information is directed; and

3 (c) the publication of the material or the uploading of the information will
4 constitute a criminal act punishable by laws enumerated in Section 6 of this Act.

5 5. No person shall be compelled to remove published material or uploaded information
6 from the Internet that is beyond the said person's capacity to remove. The party seeking to
7 compel the removal of the information has the burden to prove that the person being compelled
8 has the capacity to remove from the Internet the specific material or information. For purposes of
9 this section, material retained in web archives or mirror sites are presumed to be information that
10 is beyond the capacity of the person being compelled to remove.

11 6. The State shall not promote censorship or the restriction of the viewing of any content
12 on the Internet, until after the issuance of an appropriate Order pursuant to the provisions of this
13 Section.

14 *Section 9. Protection of the freedom to innovate and create without permission. –*

15 1. The State shall, within its jurisdiction, protect and promote the freedom to innovate
16 and create without need for permission. No person shall restrict or deny another person the right
17 to develop new information and communications technologies, without due process of law or
18 authority vested by law.

19 2. Subject to such conditions as provided for in the Intellectual Property Code and other
20 relevant laws, no person shall be denied access to new information and communications
21 technologies, nor shall any new information and communications technologies be blocked,
22 censored, suppressed, or otherwise restricted, without due process of law or authority vested by
23 law.

24 3. No person who shall have created, invented, innovated, or otherwise developed a new
25 information and communications technology shall be penalized for the actions of the users of the
26 new information and communications technology.

1 *Section 10. Right to privacy of data. –*

2 1. The State shall, within its jurisdiction, promote the protection of the privacy of data for
3 all persons.

4 2. It shall not be unlawful for any person to employ means such as encryption or
5 cryptography to protect the privacy of the data or networks over which the person has property
6 rights over.

7 3. Subject to such conditions as provided for in the Data Privacy Act of 2012 and other
8 relevant laws, no person shall access the private data of another person.

9 4. The State shall, within its jurisdiction, protect the right of a person to ensure the
10 privacy of the data or networks over which the person has property rights over, and shall protect
11 the right of a person to employ reasonable means to this end. It shall not be unlawful for any
12 person to employ means such as encryption or cryptography to protect the privacy of the data or
13 networks over which the person has property rights over.

14 5. Agencies and instrumentalities of the State that maintain data or networks shall be
15 required to ensure the appropriate level of privacy of the data and of the networks being
16 maintained. Failure to do so shall be penalized by this Act and other relevant laws.

17 6. Except upon a final ruling from the courts, issued following due notice or hearing, may
18 a person compel an agency or instrumentality of the State maintaining data or networks to reduce
19 the level of privacy of the data or of the networks.

20 *Section 11. Right to security of data. –*

21 1. The State shall, within its jurisdiction, promote the protection of the security of data for
22 all persons.

23 2. It shall not be unlawful for any person to employ any means, whether physical,
24 electronic, or behavioral, to protect the security of the data or networks over which the person
25 has property rights over.

26 3. Subject only to such conditions as provided for in the Data Privacy Act and other
27 relevant laws, and upon a final ruling from the courts, issued following due notice and hearing,
28 may an Internet service provider, telecommunications entity, or other such persons providing

1 Internet or data services, be compelled to provide a third party access to the private data or
2 networks of, belonging to, or otherwise identified with another person. The Internet service
3 provider, telecommunications entity, or such person providing Internet or data services is
4 obligated to notify the person that a third party has been granted access to the private data or
5 networks of the person, before the third party shall access the private data or networks of the
6 person.

7 4. No third party shall be granted access to the private data or networks of a person by an
8 Internet service provider, telecommunications entity, or such person providing Internet or data
9 services if the person has not been properly notified that a request for access to the private data
10 or networks of the person has been made. A person shall not be deemed to have been properly
11 notified unless the person has acknowledged the notification of the request for access and has
12 agreed to grant or refuse access, or unless an order compelling the person to grant the third party
13 access to the private data or networks shall be issued by a competent court having jurisdiction
14 over the residence of the person, following due notice and hearing.

15 5. No third party granted the right to access the private data or networks of a person by an
16 Internet service provider, telecommunications entity, or other such person providing Internet or
17 data services, shall be given any property rights over the data being accessed, the media where
18 the private data is stored, the equipment through which the network is run or maintained, or the
19 physical plant where the network equipment is housed, beyond the right to access the private
20 data or network. Only upon a separate final ruling from the courts, issued following due notice
21 and hearing, shall the third party have any property rights supplementary to the right to access the
22 private data or network.

23 6. Except upon a final ruling from the courts, issued following due notice and hearing,
24 that the data, information, or contents of a device, network equipment, or physical plant that is
25 the subject of judicial or quasi-judicial proceedings cannot be separated from the device, network
26 equipment, or physical plant, no device, network equipment, or physical plant shall be seized as
27 evidence of violation of this Act or other relevant laws. Except if seizure will cause restriction or
28 stoppage of legitimate Internet or network operations that are not subject to judicial or quasi-

1 judicial proceedings, storage media may be seized as evidence in accordance with the Rules of
2 Court.

3 7. Agencies and instrumentalities of the State that maintain data or networks, whether
4 private or public, shall be required to ensure the appropriate level of security of the data and of
5 the networks being maintained. Failure to do so shall be penalized by this Act and other relevant
6 laws.

7 8. No person may compel an agency or instrumentality of the State maintaining data or
8 networks to reduce the level of security of the data or of the networks being maintained.

9 *Section 12. Protection of intellectual property. –*

10 1. The State shall, within its jurisdiction, protect the intellectual property published on the
11 Internet of all persons, subject to such conditions as provided for in the Intellectual Property
12 Code and other relevant laws.

13 2. It shall be presumed that any content published on the Internet is copyrighted, unless
14 otherwise explicitly provided for by the author, subject to such conditions as provided for in the
15 Intellectual Property Code and other relevant laws.

16 3. Subject to Republic Act No. 8293 aka the “Intellectual Property Code of the
17 Philippines” and other relevant laws, no Internet Service Provider, telecommunications entity, or
18 such person providing Internet or data services shall have intellectual property rights over
19 derivative content that is the result of creation, invention, innovation, or modification by a person
20 using the service provided by the Internet service provider, telecommunications entity, or such
21 person providing Internet or data services, unless such content is a derivative work of content
22 already owned by or assigned to the Internet service provider, telecommunications entity, or such
23 person providing Internet or data services acting as a content provider. The exception to the
24 intellectual property rights of the person must be explicitly provided for via an end user license
25 agreement to which both parties have agreed, and the existence of the derivative content must be
26 dependent on the service provided by the Internet service provider, telecommunications entity, or
27 such person providing Internet or data services.

1 on the Rights of the Child (CRC), the Convention on the Elimination of All Forms of Racial
2 Discrimination (ICERD), the Convention on the Elimination of All Forms of Discrimination
3 Against Women (CEDAW), the Convention on the Rights of Persons with Disabilities (CRPD),
4 the United Nations Convention against Transnational Organized Crime, the United Nations
5 Convention against Corruption, the Geneva Convention, the United Nations Convention on
6 Certain Conventional Weapons, the Rome Statute of the International Criminal Court, the
7 Convention on Cybercrime (Budapest Convention), and the General Agreement on Tariffs and
8 Trade (GATT), among others. No agency or instrumentality of the State shall issue rules and
9 regulations governing the use of networks and the Internet contrary to these.

10 **Chapter V. Duties Related to the Promotion of Internet Freedom.**

11 *Section 15. The State as the Primary Duty Bearer. --*

12 1. The State, as the primary duty-bearer, shall uphold constitutional rights, privileges,
13 guarantees, and obligations in the development and implementation of policies related to the
14 Internet and information and communication technology.

15 2. The State shall fulfill this duty through law, policy, regulatory instruments,
16 administrative guidelines, and other appropriate measures, including temporary special measures.

17 3. The State shall keep abreast with and be guided by developments of the Internet and of
18 information and communications technology under international law and shall continually design
19 and implement policies, laws, and other measures to promote the objectives of this Act.

20 *Section 16. Duties of the State Agencies and Instrumentalities. --*

21 *A. Oversight*

22 A. 1. Subject to provisions of this Act, the Department of Information and
23 Communications Technology (DICT) shall be the lead agency for oversight over the
24 development and implementation of plans, policies, programs, measures, and
25 mechanisms in the use of the Internet and information and communications technology in
26 the Philippines.

1 A. 2. The National Telecommunications Commission or its successor agency shall
2 be attached to the DICT. It shall be responsible for the development, implementation, and
3 enforcement of regulations, standards, instructions, and orders governing ICT
4 infrastructure. The NTC shall be responsible for dispute resolution, and administrative
5 and quasi-judicial proceedings, in the event of civil violations of this Act.

6 A. 3. The National Data Privacy Commission, as provided for by the Data Privacy
7 Act of 2012, as amended, shall be attached to the DICT. It shall be responsible for the
8 development, implementation, and enforcement of regulations, standards, instructions,
9 and orders governing data privacy and security. The NDPC shall be responsible for
10 dispute resolution, and administrative and quasi-judicial proceedings, in the event of civil
11 violations of this Act.

12 A. 4. The DICT shall establish an ICT Legal Affairs Office, independent of the
13 NTC and the NDPC, and independent of its other offices. The ICT Legal Affairs office
14 shall be responsible for providing technical assistance to state prosecutors in the event of
15 violations of this Act, and shall be responsible for the filing of cases against persons
16 performing violations of this Act, upon recommendation by the NTC and the NDPC.

17 A. 5. The Telecommunications Office or its successor agency shall be attached to
18 the DICT. It shall be responsible for development of national ICT infrastructure primarily
19 in and up to unserved and underserved areas, and the promotion of the use of ICT
20 infrastructure in unserved and underserved areas. The President may, at his discretion,
21 dissolve the Telecommunications Office for reasons of underperformance or
22 nonperformance.

23 A. 6. The National Computer Center and the National Telecommunications
24 Training Institute shall be combined into the National Information and Communications
25 Technology Institute (NICTI). The NICTI shall be attached to the DICT, and shall be
26 primarily responsible for the development, discretion, and control of information and
27 communications technology as a national resource, such as the acquisition and utilization
28 of computers and related devices, data communications, information systems, software
29 development, and manpower development. It shall be tasked to coordinate all activities

1 related to information technology development in the country, and shall be primarily
2 responsible for the training of government personnel in information and communications
3 technology. The NICTI shall also be tasked to ensure the implementation of an integrated
4 national information and communications technology program.

5 The President may, at his discretion, dissolve the National Information and
6 Communications Technology Institute for reasons of underperformance or
7 nonperformance.

8 A. 7. The DICT and the Official Gazette may establish a clearinghouse for
9 government public information, with the responsibility of publishing online and
10 periodically updating government public information, to promote transparency and
11 citizen engagement through the use of information and communications technology.

12 *B. Cybercrime Law Enforcement.* – Subject to provisions of this Act, the Department of
13 Justice, The Department of Interior and Local Government, the Department of Social Welfare
14 and Development, the Department of Information and Communications Technology, the
15 National Bureau of Investigation, and the Philippine National Police shall be jointly responsible
16 over the development and implementation of plans, policies, programs, measures, and
17 mechanisms for cybercrime law enforcement in the Philippines.

18 *C. Cyberdefense and Cybersecurity.* – Subject to provisions of this Act, the Department
19 of National Defense shall be the lead agency for oversight over the development and
20 implementation of plans, policies, programs, measures, mechanisms, and weapons for national
21 cyberdefense and cybersecurity.

22 *D. Information and Communications Technology Infrastructure Development.* –

23 D. 1. Subject to provisions of this Act, the Department of Information and
24 Communications Technology and the National Economic and Development Authority
25 shall have the joint responsibility to develop and implement plans, policies, programs,
26 measures, and mechanisms for the development of information and communications

1 technology infrastructure in the Philippines and the promotion of investment
2 opportunities to this end.

3 D. 2. Entities involved in the development and operation of information and
4 communications technology infrastructure and facilities shall be entitled to the following
5 incentives upon registration with the Board of Investments:

6 a) Income Tax Holiday for a period no greater than the first five (5) years
7 of commercial operation.

8 b) Duty-free importation of machinery, equipment, and materials within
9 five (5) years from registration, provided that the importations entitled to the
10 incentive shall be those directly and actually needed and used exclusively for the
11 information and communications technology facilities and services.

12 c) Special realty tax rates on civil works, equipment, machinery and other
13 improvements actually and exclusively used for information and communications
14 technology facilities and services.

15 d) Net operating loss carry-over (NOLCO) during the first three years
16 from the start of commercial operations that have not been previously offset as
17 deduction from gross income shall be carried over for the next three (3)
18 consecutive taxable years immediately following the year of such loss, provided
19 that operating loss resulting from the availment of incentives under this Act shall
20 not be entitled to NOLCO.

21 e) Special corporate tax rate of ten percent (10%) on its net taxable
22 income, which shall take effect upon the expiration of the five (5) years income
23 tax holiday, for a period no greater than five (5) years.

24 f) Tax credit for entities involved in the development of information and
25 communications technology infrastructure and facilities for missionary network
26 connectivity in areas identified by the Telecommunications Office as unserved or
27 underserved.

28 g) Tax credit on domestic capital equipment and services equivalent to one
29 hundred percent (100%) of the value of the value-added tax and customs duties

1 that would have been paid on the information and communications machinery and
2 equipment had these been imported shall be given to a registered entity who
3 purchases the same from a domestic manufacturer.

4 h) The implementing rules of the registration of the entity involved in the
5 development or operation information and communications technology as well as
6 the incentives provided herein shall be developed by the Board of Investments
7 together with the DICT and the Department of Finance.

8 i) The information and communications technology sector is hereby
9 declared a priority investment sector and shall regularly form part of the country's
10 Investment Priority Plan. All entities involved in the development or operation
11 information and communications technology registered with the BOI under this
12 Act shall be entitled to the incentives provided herein and in the IPP.

13 D. 3. Subject to joint oversight by the DICT, the DOF, the Department of Budget
14 and Management, and the Commission on Audit, the NEDA may establish a venture
15 capital corporation to encourage research and development of information and
16 communications technology in the Philippines.

17 *E. Human Resources, Skills and Technology Development for Information and*
18 *Communications Technology.* – Subject to provisions of this Act, the Department of Information
19 and Communications Technology, the Department of Science and Technology, and the
20 Technical Education and Skills Development Authority shall have the joint responsibility to
21 develop and implement plans, policies, programs, measures, and mechanisms for the
22 development of human resources, skills development, and technology development for
23 information and communications technology infrastructure in the Philippines.

24 *F. Information and Communications Technology Education.* – Subject to provisions of
25 this Act, the Department of Information and Communications Technology, the Department of
26 Education, and the Commission on Higher Education shall have the joint responsibility to
27 develop and implement plans, policies, programs, measures, and mechanisms for information
28 and communications technology education in the Philippines.

1 *G. Intellectual Property Rights Protection in Cyberspace.* – Subject to provisions of this
2 Act and other relevant laws, the Intellectual Property Office shall, within Philippine jurisdiction,
3 be primarily responsible for the protection of intellectual property rights in cyberspace. As
4 official registrar and repository of copies of published works, the National Library and the
5 National Archives shall assist the Intellectual Property Office in the protection of copyright.

6 **Chapter VI. Regulations for the Promotion of Internet Rights and Freedoms.**

7 *Section 17. Amendments to the Public Telecommunications Policy Act of the Philippines.*

8 –

9 1. Article III, Section 5 of Republic Act No. 7925 aka the “Public Telecommunications
10 Policy Act of the Philippines” is hereby amended to read:

11 *Section 5. Responsibilities of the National Telecommunications*
12 *Commission.* - The National Telecommunications Commission (Commission)
13 shall be the principal administrator of this Act and as such shall take the necessary
14 measures to implement the policies and objectives set forth in this Act.
15 Accordingly, in addition to its existing functions, the Commission shall be
16 responsible for the following:

17 a) Adopt an administrative process which would facilitate the entry of
18 qualified service providers and adopt a pricing policy which would generate
19 sufficient returns to encourage them to provide basic telecommunications,
20 **NETWORK, AND INTERNET** services in unserved and underserved areas;

21 b) Ensure quality, safety, reliability, security, compatibility and inter-
22 operability of telecommunications, **NETWORK, AND INTERNET**
23 **FACILITIES** and services in conformity with standards and specifications set by
24 international radio, telecommunications, **NETWORK, AND INTERNET**
25 organizations to which the Philippines is a signatory;

26 c) Mandate a fair and reasonable interconnection of facilities of
27 authorized public network operators and other providers of telecommunications,
28 **NETWORK, AND INTERNET** services through appropriate modalities of

1 interconnection and at a reasonable and fair level of charges, which make
2 provision for the cross subsidy to unprofitable local exchange service areas so as
3 to promote telephone [density], **MOBILE PHONE, NETWORK, AND**
4 **BROADBAND DENSITY** and provide the most extensive access to basic
5 telecommunications, **NETWORK, AND INTERNET** services available at
6 affordable rates to the public;

7 d) Foster fair and efficient market conduct through, but not limited to the
8 protection of telecommunications entities from unfair trade practices of other
9 carriers;

10 e) Promote consumers' welfare by facilitating access to
11 telecommunications, **NETWORK, AND INTERNET SERVICES** whose
12 infrastructure and network must be geared towards the needs of individual and
13 business users, **AND BY DEVELOPING AND IMPLEMENTING**
14 **STANDARDS, PLANS, POLICIES, PROGRAMS, MEASURES, AND**
15 **MECHANISMS, INCLUDING ARBITRATION, QUASI-JUDICIAL, AND**
16 **PROSECUTORIAL MECHANISMS, TO PROTECT THE WELFARE OF**
17 **CONSUMERS AND USERS OF TELECOMMUNICATIONS, NETWORK,**
18 **AND INTERNET SERVICES;**

19 f) Protect consumers against misuse of a telecommunications entity's
20 monopoly or quasi-monopolistic powers by, but not limited to, the investigation
21 of complaints and exacting compliance with service standards from such entity;
22 and

23 g) In the exercise of its regulatory and powers, continue to impose such
24 fees and charges as may be necessary to cover reasonable costs and expenses for
25 the regulation and supervision of the operations of telecommunications entities.

26 2. Article III, Section 6 of the Public Telecommunications Policy Act of the Philippines is
27 hereby amended to read:

1 *Section 6. Responsibilities of and Limitations to Department Powers. -*

2 The Department of [Transportation and Communications (DOTC)]
3 **INFORMATION AND COMMUNICATIONS TECHNOLOGY (DICT)** shall
4 not exercise any power which will tend to influence or effect a review or a
5 modification of the Commission's quasi-judicial functions.

6 In coordination with the Commission, however, the Department shall, in
7 accordance with the policies enunciated in this Act, be responsible for:

8 a) the development and maintenance of a long-term strategic national
9 development plan for to serve as a guide to the industry and potential investors as
10 well as to the Commission;

11 b) the coordination of research and development activities in government
12 with the work of other institutions in the field of information and communications
13 technology;

14 c) the representation and promotion of Philippine interests in international
15 bodies, and the negotiation of the nation's rights and obligations in international
16 [telecommunications] **INFORMATION TECHNOLOGY,**
17 **COMMUNICATIONS, NETWORK, AND INTERNET** matters; and

18 d) the operation of a national consultative forum to facilitate interaction
19 amongst the [telecommunications industries] **INFORMATION,**
20 **COMMUNICATIONS, NETWORK, AND INTERNET INDUSTRIES,**
21 **USER GROUPS,** academic and research institutions in the airing and resolution
22 of important issues in the field of [communications]
23 **TELECOMMUNICATIONS AND THE INTERNET.**

24 3. Article IV of the Public Telecommunications Policy Act of the Philippines is hereby
25 amended to include the following provisions:

26 **SECTION 11. LOCAL INTERNET SERVICE PROVIDER. – A LOCAL**
27 **INTERNET SERVICE PROVIDER SHALL:**

1 (A) PROVIDE UNIVERSAL INTERNET CONNECTION SERVICE
2 TO ALL SUBSCRIBERS WHO APPLIED FOR SUCH SERVICE, WITHIN A
3 REASONABLE PERIOD AND AT SUCH STANDARDS AS MAY BE
4 PRESCRIBED BY THE COMMISSION AND AT SUCH TARIFF AS TO
5 SUFFICIENTLY GIVE IT A FAIR RETURN ON ITS INVESTMENTS.

6 (B) BE PROTECTED FROM UNCOMPENSATED BYPASS OR
7 OVERLAPPING OPERATIONS OF OTHER TELECOMMUNICATIONS
8 ENTITIES IN NEED OF PHYSICAL LINKS OR CONNECTIONS TO ITS
9 CUSTOMERS IN THE AREA EXCEPT WHEN IT IS UNABLE TO
10 PROVIDE, WITHIN A REASONABLE PERIOD OF TIME AND AT
11 DESIRED STANDARD, THE INTERCONNECTION ARRANGEMENTS
12 REQUIRED BY SUCH ENTITIES.

13 (C) HAVE THE FIRST OPTION TO PROVIDE PUBLIC OR
14 PRIVATE NETWORK ACCESS OR INTERNET ACCESS NODES OR
15 ZONES IN THE AREA COVERED BY ITS NETWORK.

16 (D) BE ENTITLED TO A FAIR AND EQUITABLE REVENUE
17 SHARING ARRANGEMENT WITH THE INTERNET EXCHANGE,
18 INTERNET DATA CENTER, INTERNET GATEWAY FACILITY, OR SUCH
19 OTHER CARRIERS CONNECTED TO ITS BASIC NETWORK.

20 PROVIDED THAT THE SERVICE IT PROVIDES IS SOLELY
21 DEPENDENT ON EXISTING NETWORKS BEING OPERATED AND
22 MAINTAINED BY AT LEAST ONE OTHER TELECOMMUNICATIONS
23 ENTITY, A LOCAL INTERNET SERVICE PROVIDER NEED NOT SECURE
24 A FRANCHISE.

25 A CABLE TV FRANCHISE MAY PROVIDE LOCAL INTERNET
26 CONNECTION, NETWORK, OR DATA TRANSMISSION SERVICES
27 WITHOUT A SEPARATE FRANCHISE; PROVIDED, THAT THE
28 OPERATION OF INTERNET CONNECTION, NETWORK, OR DATA
29 TRANSMISSION SERVICE BY THE CABLE TV FRANCHISE SHALL BE
30 GOVERNED BY THIS ACT AND OTHER RELEVANT LAWS.

1 THE PROVISION OF INTERNET CONNECTION, NETWORK, OR
2 DATA TRANSMISSION SERVICES SHALL BE ALSO BE GOVERNED BY
3 THE PUBLIC SERVICE ACT, AS AMENDED, AND OTHER RELEVANT
4 LAWS GOVERNING UTILITIES.

5 *SECTION 12. INTERNET EXCHANGE.* - THE NUMBER OF
6 ENTITIES ALLOWED TO PROVIDE INTERNET EXCHANGE SERVICES
7 SHALL NOT BE LIMITED, AND AS A MATTER OF POLICY, WHERE IT
8 IS ECONOMICALLY VIABLE, AT LEAST TWO (2) INTERNET
9 EXCHANGES SHALL BE AUTHORIZED: PROVIDED, HOWEVER, THAT
10 A LOCAL INTERNET SERVICE PROVIDER SHALL NOT BE
11 RESTRICTED FROM OPERATING ITS OWN INTERNET EXCHANGE
12 SERVICE IF ITS VIABILITY IS DEPENDENT THERETO. SUCH
13 INTERNET EXCHANGE SHALL HAVE THE FOLLOWING
14 OBLIGATIONS:

15 (A) IT SHALL INTERCONNECT WITH ALL OTHER INTERNET
16 EXCHANGES IN THE SAME CATEGORY AND WITH ALL LOCAL
17 INTERNET SERVICE PROVIDERS AND OTHER
18 TELECOMMUNICATIONS ENTITIES, UPON APPLICATION AND
19 WITHIN A REASONABLE TIME PERIOD, AND UNDER FAIR AND
20 REASONABLE LEVEL CHARGES, IN ORDER THAT INTERNET AND
21 NETWORK SERVICES ARE MADE POSSIBLE; AND

22 (B) IT SHALL HAVE THE RIGHT TO ESTABLISH AND OPERATE
23 ITS OWN NETWORK FACILITIES THROUGH WHICH INTERNATIONAL
24 NETWORKS OR INTERNATIONAL GATEWAY FACILITIES SHALL BE
25 ABLE TO COURSE THEIR MESSAGES OR SIGNALS.

26 (C) IT SHALL COMPLY WITH INTERNATIONAL AND GENERIC
27 ENGINEERING REQUIREMENTS AND STANDARDS OF OPERATION
28 FOR INTERNET EXCHANGES.

29 *SECTION 13. INTERNET DATA CENTER.* - THE NUMBER OF
30 ENTITIES ALLOWED TO PROVIDE INTERNET DATA CENTER

1 SERVICES SHALL NOT BE LIMITED, AND AS A MATTER OF POLICY,
2 WHERE IT IS ECONOMICALLY VIABLE, AT LEAST TWO (2) INTERNET
3 DATA CENTERS SHALL BE AUTHORIZED: PROVIDED, HOWEVER,
4 THAT A LOCAL INTERNET SERVICE PROVIDER OR CONTENT
5 PROVIDER SHALL NOT BE RESTRICTED FROM OPERATING ITS OWN
6 INTERNET DATA CENTER IF ITS VIABILITY IS DEPENDENT
7 THERETO. SUCH INTERNET DATA CENTER SHALL HAVE THE
8 FOLLOWING OBLIGATIONS:

9 (A) IT SHALL INTERCONNECT WITH ALL OTHER INTERNET
10 DATA CENTERS IN THE SAME CATEGORY AND WITH ALL LOCAL
11 INTERNET SERVICE PROVIDERS AND OTHER
12 TELECOMMUNICATIONS ENTITIES, UPON APPLICATION AND
13 WITHIN A REASONABLE TIME PERIOD, AND UNDER FAIR AND
14 REASONABLE LEVEL CHARGES, IN ORDER THAT INTERNET AND
15 NETWORK SERVICES ARE MADE POSSIBLE; AND

16 (B) IT SHALL HAVE THE RIGHT TO ESTABLISH AND OPERATE
17 ITS OWN NETWORK FACILITIES THROUGH WHICH INTERNATIONAL
18 NETWORKS OR INTERNATIONAL GATEWAY FACILITIES SHALL BE
19 ABLE TO COURSE THEIR MESSAGES OR SIGNALS.

20 (C) IT SHALL COMPLY WITH INTERNATIONAL AND GENERIC
21 ENGINEERING REQUIREMENTS AND STANDARDS OF OPERATION
22 FOR NETWORK AND DATA CENTERS.

23 *SECTION 14. INTERNET GATEWAY FACILITY.* – ONLY ENTITIES
24 WHICH WILL PROVIDE INTERNET EXCHANGE SERVICES OR
25 INTERNET DATA CENTER SERVICES, AND CAN DEMONSTRABLY
26 SHOW TECHNICAL AND FINANCIAL CAPABILITY TO INSTALL AND
27 OPERATE AN INTERNATIONAL GATEWAY FACILITY, SHALL BE
28 ALLOWED TO OPERATE AS AN INTERNET GATEWAY FACILITY.

29 THE ENTITY SO ALLOWED SHALL BE REQUIRED TO PRODUCE
30 A FIRM CORRESPONDENT OR INTERCONNECTION RELATIONSHIPS

1 WITH MAJOR OVERSEAS TELECOMMUNICATIONS AUTHORITIES,
2 CARRIERS, OVERSEAS INTERNET GATEWAYS, NETWORKS, AND
3 INTERNET SERVICE PROVIDERS WITHIN ONE (1) YEAR FROM THE
4 GRANT OF THE AUTHORITY.

5 THE INTERNET GATEWAY FACILITY SHALL ALSO COMPLY
6 WITH ITS OBLIGATIONS TO PROVIDE INTERNET EXCHANGE
7 SERVICES IN UNSERVED OR UNDERSERVED AREAS WITHIN THREE
8 (3) YEARS FROM THE GRANT OF THE AUTHORITY AS REQUIRED BY
9 EXISTING REGULATIONS: PROVIDED, HOWEVER, THAT SAID
10 INTERNET GATEWAY FACILITY SHALL BE DEEMED TO HAVE
11 COMPLIED WITH THE SAID OBLIGATION IN THE EVENT IT ALLOWS
12 AN AFFILIATE THEREOF TO ASSUME SUCH OBLIGATION AND WHO
13 COMPLIES THEREWITH.

14 FAILURE TO COMPLY WITH THE ABOVE OBLIGATIONS SHALL
15 BE A CAUSE TO CANCEL ITS AUTHORITY OR PERMIT TO OPERATE
16 AS AN INTERNET GATEWAY FACILITY.

17 *SECTION 15. CONTENT PROVIDER.* – EXCEPT FOR BUSINESS
18 PERMITS AND OTHER REGULATORY REQUIREMENTS AS PROVIDED
19 FOR BY THE CONSUMER ACT OF THE PHILIPPINES, AS AMENDED,
20 AND OTHER RELEVANT LAWS, AND PROVIDED THAT THE
21 TRANSMISSION OF ITS CONTENT IS SOLELY DEPENDENT ON
22 EXISTING NETWORKS BEING OPERATED AND MAINTAINED BY AT
23 LEAST ONE OTHER TELECOMMUNICATIONS ENTITY, A CONTENT
24 PROVIDER FOR COMMERCIAL OR NON-COMMERCIAL PURPOSES
25 NEED NOT SECURE A FRANCHISE, LICENSE, OR PERMIT TO
26 OPERATE IN THE PHILIPPINES.

27 SUBJECT TO THE NATURE OF THE CONTENT THAT IS
28 PROVIDED BY THE CONTENT PROVIDER FOR COMMERCIAL
29 PURPOSES, LAWS SUCH AS PAGCOR CHARTER, AS AMENDED, THE

1 MTRCB CHARTER, AS AMENDED, AND OTHER RELEVANT LAWS,
2 SHALL BE DEEMED APPLICABLE TO THE CONTENT PROVIDER.

3 4. Article IV, Section 11 of the Public Telecommunications Policy Act of the Philippines
4 is hereby amended to read:

5 *Section 11. Value-added Service Provider.* – Provided that [it does not put
6 up its own network] **THE SERVICE IT PROVIDES IS SOLELY**
7 **DEPENDENT ON EXISTING NETWORKS BEING OPERATED AND**
8 **MAINTAINED BY AT LEAST ONE OTHER TELECOMMUNICATIONS**
9 **ENTITY**, a VAS provider need not secure a franchise. A VAS provider shall be
10 allowed to competitively offer its services and/or expertise, and lease or rent
11 telecommunications equipment and facilities necessary to provide such
12 specialized services, in the domestic and/or international market in accordance
13 with network compatibility.

14 Telecommunications entities may provide VAS, subject to the additional
15 requirements that:

16 (a) prior approval of the Commission is secured to ensure that such VAS
17 offerings are not cross-subsidized from the proceeds of their utility operations;

18 (b) other providers of VAS are not discriminated against in rates nor
19 denied equitable access to their facilities; and,

20 (c) separate books of accounts are maintained for the VAS.

21 **THE PROVISION OF HIGH-SPEED OR HIGH-VOLUME**
22 **INTERNET CONNECTION OR DATA TRANSMISSION SERVICES AS A**
23 **SERVICE SEPARATE FROM NORMAL INTERNET CONNECTION OR**
24 **DATA TRANSMISSION SERVICES SHALL NOT BE CLASSED AS A**
25 **VALUE-ADDED SERVICE.**

26 5. Article V, Section 14 of the Public Telecommunications Policy Act of the Philippines
27 is hereby amended to read:

1 *Section 14. Customer Premises Equipment.* – Telecommunications
2 subscribers **AND INTERNET AND NETWORK USERS** shall be allowed to
3 use within their premises terminal equipment, such as telephone, PABX,
4 facsimile, **SUBSCRIBER IDENTIFICATION MODULE (SIM) CARDS**,
5 data, record, message and other special purpose or multi-function
6 telecommunication terminal equipment intended for such connection: Provided,
7 that the equipment is type-approved by the Commission.

8 **UNLESS DESIGNED AND MANUFACTURED AS SUCH**
9 **WITHOUT NEED FOR A SPECIAL REQUEST BY A**
10 **TELECOMMUNICATIONS ENTITY, NO CUSTOMER PREMISES**
11 **EQUIPMENT SHALL BE RESTRICTED FROM INTERCONNECTING**
12 **TO A NETWORK OR TO THE INTERNET, OR INTEROPERABILITY**
13 **WITH OTHER CUSTOMER PREMISES EQUIPMENT, NETWORK**
14 **EQUIPMENT, DATA STORAGE EQUIPMENT, OR OTHER DEVICES**
15 **OR EQUIPMENT THAT MAY BE NORMALLY INTERCONNECTED**
16 **WITH OR MAY NORMALLY ENJOY INTEROPERABILITY WITH, AS**
17 **APPLICABLE; PROVIDED, HOWEVER, THAT IN THE COURSE OF**
18 **NORMAL OPERATIONS SUCH INTERCONNECTION OR**
19 **INTEROPERABILITY SHALL NOT COMPROMISE DATA OR**
20 **NETWORK PRIVACY OR SECURITY.**

21 6. Article VII, Section 20 of The Public Telecommunications Policy Act of the
22 Philippines is hereby amended to read:

23 *Section 20. Rights of End-Users.* – The user of telecommunications,
24 **INTERNET, NETWORK, OR DATA TRANSMISSION** service shall have the
25 following basic rights:

26 (a) Entitlement of utility service which is non-discriminatory, reliable and
27 conforming with minimum standards set by the Commission;

28 (b) Right to be given the first single-line telephone connection or the first
29 party-line connection within two (2) months of application for service, against

1 deposit; or within three (3) months after targeted commencement of service in the
2 barangay concerned per the original schedule of service expansion approved by
3 the Commission, whichever deadline comes later;

4 **(C) RIGHT TO BE GIVEN THE FIRST INTERNET OR**
5 **NETWORK CONNECTION WITHIN TWO (2) MONTHS OF**
6 **APPLICATION FOR SERVICE, AGAINST DEPOSIT; OR WITHIN**
7 **THREE (3) MONTHS AFTER TARGETED COMMENCEMENT OF**
8 **SERVICE IN THE BARANGAY CONCERNED PER THE ORIGINAL**
9 **SCHEDULE OF SERVICE EXPANSION APPROVED BY THE**
10 **COMMISSION, WHICHEVER DEADLINE COMES LATER;**

11 (d) Regular, timely and accurate billing, courteous and efficient service at
12 utility business offices and by utility company personnel;

13 **(E) TIMELY CORRECTION OF ERRORS IN BILLING AND THE**
14 **IMMEDIATE PROVISION OF REBATES OR REFUNDS BY THE**
15 **UTILITY WITHOUT NEED FOR DEMAND BY THE USER; AND;**

16 (f) Thorough and prompt investigation of, and action upon complaints.
17 The utility shall endeavor to allow complaints [over the telephone] **TO BE**
18 **RECEIVED. BY POST AND OVER MEANS USING**
19 **TELECOMMUNICATIONS FACILITIES OR THE INTERNET, WHICH**
20 **SHALL INCLUDE BUT SHALL NOT BE LIMITED TO VOICE CALLS,**
21 **SHORT MESSAGE SERVICE (SMS) MESSAGES, MULTIMEDIA**
22 **MESSAGE SERVICE (MMS) MESSAGES, OR EMAIL,** and shall keep a
23 record of all [written or phoned-in] complaints received and the actions taken to
24 address these complaints;

25 **SUBJECT TO THE FILING OF A FORMAL REQUEST TO THE**
26 **UTILITY, A USER MAY REQUEST THE IMMEDIATE TERMINATION**
27 **OF SERVICE, WITHOUT THE IMPOSITION OF FEES OR PENALTIES,**
28 **AND WITH THE REFUND OF ANY FEES OR CHARGES ALREADY**
29 **PAID BY THE USER, SHOULD A UTILITY NOT CONSISTENTLY**

1 COMPLY WITH PRECEDING PARAGRAPHS (A), (D), (E), (F), OR ANY
2 OTHER MINIMUM PERFORMANCE STANDARDS SET BY THE
3 COMMISSION.

4 SUBJECT TO STANDARDS SET BY THE COMMISSION,
5 REASONABLE FEES OR PENALTIES MAY BE IMPOSED BY THE
6 UTILITY, OR MAY BE DEDUCTED FROM ANY FEES OR CHARGES
7 ALREADY PAID BY THE USER, SHOULD A USER REQUEST THE
8 IMMEDIATE TERMINATION OF SERVICE; PROVIDED THAT:

9 (1) THE UTILITY IS ABLE TO SHOW THAT THE REQUEST IS
10 NOT BASED ON A NONCOMPLIANCE WITH PRECEDING
11 PARAGRAPHS (A), (D), (E), (F), OR ANY OTHER MINIMUM
12 PERFORMANCE STANDARDS SET BY THE COMMISSION; OR,

13 (2) THE UTILITY HAS EVIDENCE THAT THE NON-
14 COMPLIANCE HAS NOT RECURRED, IS NOT RECURRING, NOR
15 WILL RECUR IN THE FUTURE; OR THE UTILITY HAS EVIDENCE
16 THAT THE NONCOMPLIANCE WAS DUE TO FACTORS BEYOND ITS
17 CONTROL; OR THE UTILITY HAS PROVIDED IMMEDIATE REFUND
18 OR REBATE TO THE USER UPON DETECTION OF THE
19 NONCOMPLIANCE; OR THE UTILITY HAS EVIDENCE THAT IT HAS
20 EXERTED ITS BEST EFFORTS TO RESOLVE THE NONCOMPLIANCE
21 AND RESTORE THE SERVICE TO THE LEVEL AGREED BETWEEN
22 THE UTILITY AND THE USER WITHIN SEVEN (7) DAYS OF THE
23 REQUEST FOR IMMEDIATE TERMINATION; AND THE UTILITY
24 SHALL COMPLY WITH IMMEDIATE TERMINATION OF SERVICE,
25 WITHOUT THE IMPOSITION OF FEES OR PENALTIES, AND REFUND
26 ANY FEES OR CHARGES ALREADY PAID BY THE USER WITHOUT
27 NEED FOR DEMAND SHOULD THE SERVICE NOT BE RESTORED
28 WITHIN THE SEVEN (7) DAY PERIOD, WITHIN THREE (3) DAYS
29 AFTER THE TERMINATION OF SERVICE.

1 **SUBJECT TO STANDARDS SET BY THE COMMISSION,**
2 **PENALTIES MAY BE IMPOSED ON A UTILITY THAT IS UNABLE TO**
3 **COMPLY WITH PRECEDING PARAGRAPHS (B) AND (C). THE**
4 **COMMISSION MAY IMPOSE ADDITIONAL PENALTIES IF THE**
5 **UTILITY DOES NOT REFUND ANY DEPOSITS, FEES, OR CHARGES**
6 **ALREADY PAID BY THE USER WITHOUT NEED FOR DEMAND**
7 **WITHIN THREE (3) DAYS AFTER THE DEADLINE AGREED UPON**
8 **BETWEEN THE USER AND THE UTILITY.**

9 *Section 18. Quality of Service and Network Fair Use. –*

10 1. No Internet service provider, Internet exchange, Internet data center, Internet gateway
11 facility, telecommunications entity, or person providing Internet connection, network, or data
12 transmission services shall:

13 a) Fail to provide a service, or network services on reasonable, and
14 nondiscriminatory terms and conditions such that any person can offer or provide
15 content, applications, or services to or over the network in a manner that is at least equal
16 to the manner in which the provider or its affiliates offer content, applications, and
17 services free of any surcharge on the basis of the content, application, or service;

18 b) Refuse to interconnect facilities with other facilities of another provider of
19 network services on reasonable, and nondiscriminatory terms or conditions;

20 c) Block, impair, or discriminate against, or to interfere with the ability of any
21 person to use a network service to access, to use, to send, to receive, or to offer lawful
22 content, applications, or services over the Internet;

23 d) Impose an additional charge to avoid any conduct that is prohibited by
24 subscription;

25 e) Prohibit a user from attaching or using a device on the Internet provider's
26 network that does not physically damage or materially degrade other users' utilization of
27 the network;

1 f) Fail to clearly, and conspicuously disclose to users, in plain language, accurate
2 information concerning any terms, conditions, or limitations on the network service; or,

3 g) Impose a surcharge or other consideration for the prioritization or offer of
4 enhanced quality of service to data or protocol of a particular type, and must provide
5 equal quality of service to all data or protocol of that type regardless of origin or
6 ownership.

7 2. Nothing in this section shall be construed as to prevent an Internet service provider,
8 Internet exchange, Internet data center, Internet gateway facility, telecommunications entity, or
9 person providing Internet connection, network, or data transmission services from taking
10 reasonable and nondiscriminatory measures:

11 a) To manage the function of a network on a system-wide basis, provided that
12 such management function does not result in the discrimination between content,
13 application, or services offered by the provider or user;

14 b) To give priority to emergency communications;

15 c) To prevent a violation of law; or to comply with an order of the court enforcing
16 such law;

17 d) To offer consumer protection services such as parental controls, provided users
18 may refuse to enable such services, or opt-out; or,

19 e) To offer special promotional pricing or other marketing initiatives.

20 3. An Internet service provider, Internet exchange, Internet data center, Internet gateway
21 facility, telecommunications entity, or person providing Internet connection, network, or data
22 transmission services may provide for different levels of availability, uptime, or other service
23 quality standards set by the National Telecommunications Commission for services using
24 prepaid, postpaid, or other means of payment; Provided, that minimum levels of availability,
25 uptime, and other service quality standards set by the Commission shall not be different between
26 services using prepaid, postpaid, or other means of payment.

1 *Section 19. Amendments to the Intellectual Property Code of the Philippines. –*

2 1. Part IV, Chapter II, Section 172 of Republic Act No. 8293 aka the “Intellectual
3 Property Code of the Philippines” is hereby amended to read:

4 Section 172. *Literary and Artistic Works.* – 172.1. Literary and artistic
5 works, hereinafter referred to as "works", are original intellectual creations in the
6 literary and artistic domain protected from the moment of their creation and shall
7 include in particular:

8 (a) Books, pamphlets, articles, and other writings;

9 (b) Periodicals and newspapers;

10 (c) Lectures, sermons, addresses, dissertations prepared for oral delivery,
11 whether or not reduced in writing or other material form;

12 (d) Letters;

13 (e) Dramatic or dramatico-musical compositions; choreographic works or
14 entertainment in dumb shows;

15 (f) Musical compositions, with or without words;

16 (g) Works of drawing, painting, architecture, sculpture, engraving,
17 lithography or other works of art; models or designs for works of art;

18 (h) Original ornamental designs or models for articles of manufacture,
19 whether or not registrable as an industrial design, and other works of applied art;

20 (i) Illustrations, maps, plans, sketches, charts and three-dimensional works
21 relative to geography, topography, architecture or science;

22 (j) Drawings or plastic works of a scientific or technical character;

23 (k) Photographic works including works produced by a process analogous
24 to photography; lantern slides;

25 (l) Audiovisual works and cinematographic works and works produced by
26 a process analogous to cinematography or any process for making audio-visual
27 recordings;

28 (m) Pictorial illustrations and advertisements;

1 (n) **CODE, SCRIPTS, COMPUTER PROGRAMS, SOFTWARE**
2 **APPLICATIONS, AND OTHER SIMILAR WORK, WHETHER**
3 **EXECUTABLE IN WHOLE OR AS PART OF ANOTHER CODE,**
4 **SCRIPT, computer programs, SOFTWARE APPLICATION OR OTHER**
5 **SIMILAR WORK;**

6 (o) Other literary, scholarly, scientific and artistic works.

7
8 172.2. Works are protected by the sole fact of their creation, irrespective
9 of their mode or form of expression **OR PUBLICATION**, as well as of their
10 content, quality and purpose.

11 2. Part II, Chapter V, Section 177 of the Intellectual Property Code of the Philippines
12 shall be amended to read:

13 *Section 177. Copyright, [or] COPYLEFT, AND OTHER Economic*
14 *Rights. – THE ECONOMIC RIGHTS OVER ORIGINAL AND*
15 *DERIVATIVE LITERARY AND ARTISTIC WORKS SHALL BE ANY OF*
16 *THE FOLLOWING:*

17 **177.1 COPYRIGHT** – Subject to the provisions of Chapter VIII,
18 [copyright or] economic rights **UNDER COPYRIGHT** shall consist of the
19 exclusive right to carry out, authorize or prevent the following acts:

20 a) Reproduction of the work or substantial portion of the work;

21 b) Dramatization, translation, adaptation, abridgment, arrangement or
22 other transformation of the work;

23 c) The first public distribution of the original and each copy of the work
24 by sale or other forms of transfer of ownership;

25 d) Rental of the original or a copy of an audiovisual or cinematographic
26 work, a work embodied in a sound recording, a computer program, a compilation
27 of data and other materials or a musical work in graphic form, irrespective of the
28 ownership of the original or the copy which is the subject of the rental;

29 e) Public display of the original or a copy of the work;

- 1 f) Public performance of the work; and
- 2 g) Other communication to the public of the work.

3 **177.2. COPYLEFT – IS A TYPE OF LICENSE ON THE EXERCISE**
4 **OF ECONOMIC RIGHTS OVER ORIGINAL AND DERIVATIVE**
5 **WORKS, INCLUDING FREE AND OPEN-SOURCE SOFTWARE,**
6 **WHERE THE AUTHOR OR COPYRIGHT OWNER IRREVOCABLY**
7 **ASSIGNS TO THE PUBLIC, EITHER PARTIALLY OR FULLY, EITHER**
8 **ONE OR SEVERAL IN COMBINATION, THE RIGHT TO USE,**
9 **MODIFY, EXTEND, OR REDISTRIBUTE THE ORIGINAL WORK.**
10 **UNDER COPYLEFT, ANY AND ALL WORKS DERIVED FROM THE**
11 **ORIGINAL WORK SHALL BE COVERED BY THE SAME LICENSE AS**
12 **THE ORIGINAL WORK. DECLARATION OF A COPYLEFT LICENSE**
13 **SHALL BE SUFFICIENT IF A STATEMENT OF THE APPLICABLE**
14 **COPYLEFT LICENSE IS STIPULATED ON A COPY OF THE WORK AS**
15 **PUBLISHED.**

16 **177.3 FREE LICENSE – IS A TYPE OF LICENSE ON THE**
17 **EXERCISE OF ECONOMIC RIGHTS OVER ORIGINAL AND**
18 **DERIVATIVE WORKS WHERE THE AUTHOR OR COPYRIGHT**
19 **OWNER IRREVOCABLY ASSIGNS TO THE PUBLIC ALL THE**
20 **RIGHTS TO USE, MODIFY, EXTEND, OR REDISTRIBUTE THE**
21 **ORIGINAL WORK WITHOUT ANY RESTRICTIONS, OR WHERE THE**
22 **AUTHOR OR COPYRIGHT OWNER IRREVOCABLY DECLARES THE**
23 **WORK TO BE PUBLIC DOMAIN UNDER SECTIONS 175 AND 176 OF**
24 **THIS CODE. THE REDISTRIBUTION OF ANY MODIFIED OR**
25 **DERIVATIVE WORK SHALL NOT BE REQUIRED TO ADOPT THE**
26 **SAME LICENSE AS THE ORIGINAL WORK. DECLARATION OF A**
27 **FREE LICENSE SHALL BE SUFFICIENT IF A STATEMENT TO THE**
28 **EFFECT IS STIPULATED ON A COPY OF THE WORK AS PUBLISHED.**

1 **177.4 THE AUTHOR OR COPYRIGHT OWNER SHALL HAVE**
2 **THE OPTION TO DECLARE THE TYPE OF LICENSE OR ECONOMIC**
3 **RIGHTS THAT MAY BE EXERCISED BY THE PUBLIC IN RELATION**
4 **TO THE WORK; PROVIDED THAT, FAILURE OF THE AUTHOR OR**
5 **COPYRIGHT OWNER TO MAKE SUCH DECLARATION SHALL BE**
6 **CONSTRUED AS CLAIM OF ECONOMIC RIGHTS UNDER SECTION**
7 **177.1.**

8 3. Part II, Chapter VII, Section 180 of the Intellectual Property Code of the Philippines
9 shall be amended to read:

10 *Section 180. Rights of Assignee of Copyright.* – 180.1. The copyright
11 **UNDER SECTION 177.1** may be assigned in whole or in part. Within the scope
12 of the assignment, the assignee is entitled to all the rights and remedies which the
13 assignor had with respect to the copyright.

14 180.2. The copyright is not deemed assigned *inter vivos* in whole or in
15 part unless there is a written indication of such intention.

16 180.3. The submission of a literary, photographic or artistic work to a
17 newspaper, magazine or periodical for publication, shall constitute only a license
18 to make a single publication unless a greater right is expressly granted. **IN THE**
19 **CASE OF POSTING TO A WEBSITE OR AN ONLINE VERSION OF A**
20 **NEWSPAPER, MAGAZINE, OR PERIODICAL, ENABLING ACCESS TO**
21 **THE WHOLE OR PORTION OF THE WORK VIA AUTOMATIC**
22 **CONTENT SYNDICATION OR SEARCH RESULTS SHALL NOT**
23 **CONSTITUTE VIOLATION OF THE LICENSE UNLESS THE**
24 **CONTRARY IS EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT**
25 **BETWEEN COPYRIGHT OWNER AND PUBLISHER/HOST/SERVICE**
26 **PROVIDER.** If two (2) or more persons jointly own a copyright or any part
27 thereof, neither of the owners shall be entitled to grant licenses without the prior
28 written consent of the other owner or owners.

1 4. Part II, Chapter VII, Section 182 of the Intellectual Property Code of the Philippines
2 shall be amended to read:

3 *Section 182. Filing of Assignment or License OF COPYRIGHT.* – An
4 assignment or exclusive license may be filed in duplicate with the National
5 Library upon payment of the prescribed fee for registration in books and records
6 kept for the purpose. Upon recording, a copy of the instrument shall be returned to
7 the sender with a notation of the fact of record. Notice of the record shall be
8 published in the IPO Gazette.

9 5. Part II, Chapter VII, Section 187 of the Intellectual Property Code of the Philippines
10 shall be amended to read:

11 *Section 187. Reproduction of Published Work.* – 187.1. Subject to the
12 provisions of Section 177 [and subject to the provisions] in relation to the
13 provision of Subsection 187.2, the private reproduction of a published work in a
14 single copy, where the reproduction is made by a natural person exclusively for
15 research and private study, shall be permitted, without the authorization of the
16 owner of copyright in the work.

17 187.2. The permission granted under Subsection 187.1 shall not extend to
18 the reproduction of:

- 19 (a) A work of architecture in the form of building or other construction;
- 20 (b) An entire book, or a substantial part thereof, or of a musical work in
21 graphic form by reprographic means;
- 22 (c) A compilation of **RAW data, HAVING NOT UNDERGONE DATA**
23 **AND INFORMATION PROCESSING**, and other materials;
- 24 (d) A computer program except as provided in Section 189;
- 25 **(E) THE CONTENTS OF A WEBSITE, IF SUCH DOWNLOADING**
26 **IS FOR THE PURPOSE OF CREATING A BACK-UP COPY FOR**
27 **ARCHIVAL PURPOSES, OR EXCLUSIVELY TO TEMPORARILY**
28 **FACILITATE THE EXECUTION OF COMPUTER APPLICATIONS,**

1 SUCH AS BUT NOT LIMITED TO SEARCH ENGINES, OR
2 EXCLUSIVELY TO TEMPORARILY FACILITATE THE OPERATION
3 OF THE INTERNET OR NETWORKS, SUCH AS BUT NOT LIMITED
4 TO CACHE COPIES, OR EXCLUSIVELY FOR PURPOSES OF
5 STATISTICAL OR PERFORMANCE ANALYSIS; and,

6 (f) Any work in cases where reproduction would unreasonably conflict
7 with a normal exploitation of the work or would otherwise unreasonably prejudice
8 the legitimate interests of the author.

9 6. Part II, Chapter IX, Section 192 of the Intellectual Property Code of the Philippines
10 shall be amended to read:

11 *Section 192. Notice of [Copyright] APPLICABLE ECONOMIC*
12 ***RIGHTS.*** – Each copy of a work published or offered for sale may contain a
13 notice bearing the name of the copyright owner, and the year of its first
14 publication, and, in copies produced after the creator's death, the year of such
15 death. **IN CASE OF FAILURE OF THE COPYRIGHT OWNER TO**
16 **INDICATE THE LICENSE APPLICABLE FOR THE WORK, IT SHALL**
17 **BE PRESUMED THAT THE COPYRIGHT OWNER FULL COPYRIGHT**
18 **UNLESS INTENT TO THE CONTRARY IS PROVEN.**

19 *Section 20. Content Fair Use.* –

20 1. Subject to the provisions of the Intellectual Property Code of the Philippines, as
21 amended, and this Act and other relevant laws, the viewing of online content on any computer,
22 device, or equipment shall be considered fair use.

23 2. Subject to the provisions of the Intellectual Property Code of the Philippines, as
24 amended, this Act, and other relevant laws, the viewing, use, editing, decompiling, or
25 modification, of downloaded or otherwise offline content on any computer, device, or equipment
26 shall be considered fair use; Provided, that the derivative content resulting from editing,
27 decompiling, or modification shall be subject to the provisions of the Intellectual Property Code
28 of the Philippines, this Act, and other relevant laws governing derivative content.

1 3. It shall be presumed that any person who shall upload to, download from, edit, modify,
2 or otherwise use content on the Internet or telecommunications networks shall have done so with
3 full knowledge of the nature of the intellectual property protections applicable to the content.

4 *Section 21. Amendments to the E-Commerce Act.* – Subject to the provisions of this Act,
5 paragraphs (a) and (b) of Section 33 of Republic Act No. 8792 aka the “Electronic Commerce
6 Act of 2000” are hereby repealed.

7 *Section 22. Amendments to the Data Privacy Act.* –

8 1. Subject to the provisions of this Act, Section 7 of the Data Privacy Act of 2012 is
9 hereby amended in part to read:

10 Section 7. *Functions of the National DATA Privacy Commission.* – To
11 administer and implement the provisions of this Act, and to monitor and ensure
12 compliance of the country with international standards set for data protection,
13 there is hereby created an independent body to be known as the National **DATA**
14 Privacy Commission, which shall have the following functions:...

15 2. Subsequent mentions of “National Privacy Commission” are hereby amended to be
16 consistent with the amendment above.

17 3. Subject to the provisions of this Act, Sections 29, 31, and 32 of the Data Privacy Act of
18 2012 are repealed.

19 4. Subject to the provisions of this Act, Section 6 of the Data Privacy Act of 2012 is
20 amended to include the provisions on extraterritoriality as provided for by Section 44 of this Act.

21 5. Subject to the provisions of this Act, no other provision of the Data Privacy Act of
22 2012 is amended or repealed.

23 *Section 23. Repeal of the Cybercrime Law.* – Republic Act No. 10175 aka the
24 “Cybercrime Prevention Act of 2012” is repealed in its entirety.

1 **Part 3. Cybercrimes**

2 **Chapter VII. Cybercrimes and Other Prohibited Acts**

3 *Section 24. Network sabotage. –*

4 *A. Direct network sabotage. –* It shall be unlawful for any person to cause the stoppage or
5 degradation of Internet or network operations of another person, through electronic means,
6 through physical destruction of devices, equipment, physical plant, or telecommunications cables
7 including cable TV transmission lines and other transmission media, or through other means,
8 except if the stoppage or degradation has been done in the normal course of work or business by
9 a person authorized to stop, modify, or otherwise control network operations of the other person.

10 *B. Indirect network sabotage. –* It shall be unlawful for any person to install, infect,
11 implant, or otherwise put in a device, equipment, network, or physical plant any means of
12 performing stoppage, degradation, or modification of Internet or network operations, or data or
13 information processing, such as but not limited to bots, or to interconnect, establish, or otherwise
14 create a network of software, devices, equipment, or physical plants with the means of
15 performing stoppage, degradation, or modification of Internet or network operations, or data or
16 information processing, such as but not limited to botnets, except if the installation or
17 interconnection has been done in the normal course of work or business by a person authorized
18 to stop, modify, or otherwise control network operations or data or information processing of the
19 network.

20 *C. Criminal negligence not presumed in unintentional network sabotage. –* Except upon
21 a final ruling from the courts, issued following due notice and hearing, criminal negligence shall
22 not be presumed to be the cause of the unintentional stoppage or degradation of Internet or
23 network operations by a person authorized to stop, modify, or otherwise control network
24 operations, or by accident, unforeseen occurrences, or acts of God.

25 *Section 25. Failure to Provide Reasonable Security for Data and Networks. –*

26 *A. Failure to provide security. –* It shall be unlawful for any Internet service provider,
27 telecommunications entity, or other such person providing Internet or data services to

1 intentionally or unintentionally fail to provide appropriate levels of security for data, networks,
2 storage media where data is stored, equipment through which networks are run or maintained, or
3 the physical plant where the data or network equipment is housed.

4 *B. Negligent failure to provide security.* – Negligence resulting to acts in violation of the
5 Data Privacy Act of 2012 using a device, network equipment, or physical plant connected to the
6 Internet, public networks, private networks, or telecommunications facilities shall constitute a
7 violation of the preceding paragraph, without prejudice to prosecution under the Data Privacy
8 Act of 2012.

9 *C. Negligent failure to provide security presumed to be the result of criminal negligence.*
10 – The unintentional failure for any Internet service provider, telecommunications entity, or other
11 such person providing Internet or data services to provide appropriate levels of security for data,
12 networks, storage media where data is stored, equipment through which networks are run or
13 maintained, or the physical plant where the data or network equipment is housed shall be
14 presumed to be the result of criminal negligence, except upon a final ruling from the courts,
15 issued following due notice and hearing.

16 *Section 26. Violation of Data Privacy.* –

17 *A. Unauthorized access.* – It shall be unlawful for any person to intentionally access data,
18 networks, storage media where data is stored, equipment through which networks are run or
19 maintained, the physical plant where the data or network equipment is housed, without authority
20 granted by the Internet service provider, telecommunications entity, or other such person
21 providing Internet or data services having possession or control of the data or network, or to
22 intentionally access intellectual property published on the Internet or on other networks without
23 the consent of the person having ownership, possession, or control of the intellectual property, or
24 without legal grounds, even if access is performed without malice.

25 *B. Unauthorized modification.* – It shall be unlawful for any person to intentionally
26 modify data, networks, storage media where data is stored, equipment through which networks
27 are run or maintained, the physical plant where the data or network equipment is housed, without

1 authority granted by the Internet service provider, telecommunications entity, or other such
2 person providing Internet or data services having possession or control of the data or network, or
3 to intentionally modify intellectual property published on the Internet or on other networks
4 without the consent of the person having ownership, possession, or control of the intellectual
5 property, or without legal grounds, even if the modification is performed without malice.

6 C. *Unauthorized authorization or granting of privileges.* – It shall be unlawful for any
7 person to intentionally provide a third party authorization or privileges to access or modify data,
8 networks, storage media where data is stored, equipment through which networks are run or
9 maintained, the physical plant where the data or network equipment is housed, without authority
10 granted by the Internet service provider, telecommunications entity, or other such person
11 providing Internet or data services having possession or control of the data or network, or to
12 intentionally provide a third party authorization to access or modify intellectual property
13 published on the Internet or on other networks without the consent of the person having
14 ownership, possession, or control of the intellectual property, or without legal grounds, even if
15 the authorization to access or perform modifications was granted without malice.

16 D. *Unauthorized disclosure.* – It shall be unlawful for any authorized person to
17 intentionally disclose or cause the disclosure to a third party or to the public any private data
18 being transmitted through the Internet or through public networks, or any data being transmitted
19 through private networks, without legal grounds, even if the disclosure was done without malice.

20 E. *Violation of Data Privacy Act through ICT.* – It shall be unlawful to perform acts in
21 violation of the Data Privacy Act of 2012 using a device, network equipment, or physical plant
22 connected to the Internet, public networks, private networks, or telecommunications facilities.

23 Section 27. *Violation of Data Security.* –

24 A. *Hacking.* – It shall be unlawful for any unauthorized person to intentionally access or
25 to provide a third party with access to, or to hack or aid or abet a third party to hack into data,
26 networks, storage media where data is stored, equipment through which networks are run or
27 maintained, the physical plant where the data or network equipment is housed. The unauthorized

1 access or unauthorized act of providing a third party with access to, or the hacking into, data,
2 networks, storage media where data is stored, equipment through which networks are run or
3 maintained, the physical plant where the data or network equipment is housed shall be presumed
4 to be malicious.

5 B. *Cracking*. – It shall be unlawful for any unauthorized person to intentionally modify or
6 to crack data, networks, storage media where data is stored, equipment through which networks
7 are run or maintained, the physical plant where the data or network equipment is housed, or for
8 any unauthorized person to intentionally modify intellectual property published on the Internet or
9 on other networks. The unauthorized modification or cracking of data, networks, storage media
10 where data is stored, equipment through which networks are run or maintained, the physical
11 plant where the data or network equipment is housed, or unauthorized modification of
12 intellectual property published on the Internet or on other networks, shall be presumed to be
13 malicious.

14 C.1. *Phishing*. – It shall be unlawful for any unauthorized person to intentionally acquire
15 or to cause the unauthorized acquisition, or identity or data theft, or phishing of private data,
16 security information, or data or information used as proof of identity of another person. The
17 unauthorized acquisition or causing to acquire, or identity or data theft, or phishing of private
18 data, security information, or data or information used as proof of identity of another person shall
19 be presumed to be malicious.

20 C.2. Malicious disclosure of unwarranted or false information relative to any personal
21 information or personal sensitive information obtained by him or her as defined by Section 31 of
22 the Data Privacy Act of 2012 shall constitute phishing.

23 D. *Violation of Data Privacy Act in series or combination with hacking, cracking, or*
24 *phishing*. – It shall be unlawful to perform acts in violation of the Data Privacy Act of 2012
25 using a device, network equipment, or physical plant connected to the Internet, public networks,
26 private networks, or telecommunications facilities performed in series or combination with acts
27 prohibited by the preceding paragraphs.

1 *Section 28. Illegal and Arbitrary Seizure.* –

2 A. *Illegal Seizure.* – It shall be unlawful for any person to seize data, information, or
3 contents of a device, storage medium, network equipment, or physical plant, or to seize any
4 device, storage medium, network equipment, or physical plant connected to the Internet or to
5 telecommunications networks of another person without his consent, or to gain possession or
6 control of the intellectual property published on the Internet or on public networks of another
7 person without his consent, except upon a final ruling from the courts, issued following due
8 notice and hearing.

9 B. *Aiding and Abetting Illegal Seizure.* – It shall be unlawful for any person to aid or abet
10 the seizure of data, information, or contents of a device, storage medium, network equipment, or
11 physical plant, or to seize any device, storage medium, network equipment, or physical plant
12 connected to the Internet or to telecommunications networks of another person without his
13 consent, or to gain possession or control of the intellectual property published on the Internet or
14 on public networks of another person without his consent, except upon a final ruling from the
15 courts, issued following due notice and hearing, allowing the person to perform such seizure,
16 possession, or control.

17 C. *Arbitrary Seizure.* – It shall be unlawful for any public officer or employee to seize
18 data, information, or contents of a device, storage medium, network equipment, or physical
19 plant, or to seize any device, storage medium, network equipment, or physical plant connected to
20 the Internet or to telecommunications networks, or to gain possession or control of intellectual
21 property published on the Internet or on public networks, without legal grounds.

22 D. *Instigating Arbitrary Seizure.* – It shall be unlawful for any person to instruct a public
23 officer or employee to perform the seizure of data, information, or contents of a device, storage
24 medium, network equipment, or physical plant, or to seize any device, storage medium, network
25 equipment, or physical plant connected to the Internet or to telecommunications networks of
26 another person without his consent, or to gain possession or control of the intellectual property
27 published on the Internet or on public networks of another person without his consent, except

1 upon a final ruling from the courts, issued following due notice and hearing, providing the
2 person with authority to perform such seizure, possession, or control and delegate the same to a
3 public officer or employee with the authority to perform such seizure, possession, or control.

4 *Section 29. Infringement of Intellectual Property Rights. –*

5 A.1. *Copyright infringement.* – Subject to the Intellectual Property Code of the
6 Philippines, it shall be unlawful for any person to publish or reproduce on the Internet, in part or
7 in whole, any content that he does not have any economic rights over, or does not acknowledge
8 and comply with the terms of copyright or license governing the intellectual property rights
9 enjoyed by the content being published or reproduced, or falsely claims having intellectual
10 property rights over the content he does not own.

11 A.2. Non-attribution or plagiarism of copyleft content shall constitute
12 infringement.

13 A.3. Non-attribution or plagiarism of free license or public domain content shall
14 constitute infringement, but shall not be subject to damages.

15 A.4. Subject to the Intellectual Property Code of the Philippines, it shall be
16 unlawful for any person to reverse-engineer any whole or part of any computer program,
17 software, code, or script, whether or not executable, that is the subject of a copyright, and
18 that he does not have any property rights over, or does not acknowledge and comply with
19 the terms of copyright or license governing the intellectual property rights enjoyed by the
20 computer program being reverse-engineered.

21 B. *Piracy.* – Subject to the Intellectual Property Code of the Philippines, it shall be
22 unlawful for any person to publish and reproduce, with intent to profit, on the Internet or on or
23 through information and communications technologies, in part or in whole, any content, or
24 computer program, software, code, or script, whether or not executable, that he does not have
25 any property rights over.

26 C. *Cybersquatting.* – Subject to the Intellectual Property Code of the Philippines and
27 other relevant laws, and the Uniform Domain Name Dispute Resolution Policy of the Internet

1 Corporation for Assigned Names and Numbers (ICANN), it shall be unlawful for any person to
2 register or otherwise acquire, in bad faith to profit or to damage, a domain name that is:

3 a) Similar, identical, or confusingly similar to an existing trademark registered
4 with the appropriate government agency at the time of the domain name registration; or

5 b) Identical or in any way similar with the name of a person other than the
6 registrant, in case of a personal name.

7 D. *Unreasonable restriction of device privileges.* – Subject to Section 8 of this Act, it
8 shall be unlawful for any person engaged in the wholesale or retail of devices or equipment to,
9 by physical, electronic, or any other means, provide unreasonable restrictions on a device or
10 equipment.

11 Section 30. *Fraud via ICT.* – It shall be unlawful for any person who, by means of a
12 device, equipment, or physical plant connected to the Internet or to telecommunications
13 networks, or in connivance with a third party with access to the same, shall use the Internet or
14 telecommunications networks for the purpose of deceiving or defrauding another of money,
15 goods, or property.

16 Section 31. *ICT-Enabled Prostitution and ICT-Enabled Trafficking in Persons.* –

17 A. *ICT-Enabled Prostitution.* – It shall be unlawful for any person who, by means of a
18 device, equipment, or physical plant connected to the Internet or to telecommunications
19 networks, or in connivance with a third party with access to the same, shall use the Internet or
20 telecommunications networks for the purpose of enabling the exchange of money or
21 consideration for services of a sexual or lascivious nature, or facilitating the performance of such
22 services; Provided, the services shall be performed by one or more unwilling third-party adults
23 under threat or duress.

24 B.1. *ICT-Enabled Trafficking in Persons.* – The performance of acts prohibited by
25 Section 5 of R.A. No. 9208, or the “Anti-Trafficking in Persons Act of 2003,” as amended, by
26 means of a device, storage medium, network equipment, or physical plant connected to the
27 Internet or to telecommunications networks shall be deemed unlawful.

1 B.2. Section 5 of the Anti-Trafficking in Persons Act of 2003 shall be amended to read:

2 Section 5. *Acts that Promote Trafficking in Persons.* – The following acts
3 which promote or facilitate trafficking in persons, shall be unlawful:

4 (a) To knowingly lease or sublease, use or allow to be used any house,
5 building or establishment for the purpose of promoting trafficking in persons;

6 (b) To produce, print and issue or distribute unissued, tampered or fake
7 counseling certificates, registration stickers and certificates of any government
8 agency which issues these certificates and stickers as proof of compliance with
9 government regulatory and pre-departure requirements for the purpose of
10 promoting trafficking in persons;

11 (c) To advertise, publish, print, broadcast or distribute, or cause the
12 advertisement, publication, printing, broadcasting or distribution by any means,
13 including the use of information **AND COMMUNICATIONS** technology and
14 the Internet, of any brochure, flyer, or any propaganda material that promotes
15 trafficking in persons, **OR TO KNOWINGLY, WILLFULLY AND**
16 **INTENTIONALLY PROVIDE DEVICES, EQUIPMENT, OR PHYSICAL**
17 **PLANTS CONNECTED TO THE INTERNET OR TO**
18 **TELECOMMUNICATIONS NETWORKS, WITH THE PRIMARY**
19 **PURPOSE OF PROMOTING TRAFFICKING IN PERSONS;**

20 (d) To assist in the conduct of misrepresentation or fraud for purposes of
21 facilitating the acquisition of clearances and necessary exit documents from
22 government agencies that are mandated to provide pre-departure registration and
23 services for departing persons for the purpose of promoting trafficking in persons;

24 (e) To facilitate, assist or help in the exit and entry of persons from/to the
25 country at international and local airports, territorial boundaries and seaports who
26 are in possession of unissued, tampered or fraudulent travel documents for the
27 purpose of promoting trafficking in persons;

28 (f) To confiscate, conceal, or destroy the passport, travel documents, or
29 personal documents or belongings of trafficked persons in furtherance of

1 trafficking or to prevent them from leaving the country or seeking redress from
2 the government or appropriate agencies; and

3 (g) To knowingly benefit from, financial or otherwise, or make use of, the
4 labor or services of a person held to a condition of involuntary servitude, forced
5 labor, or slavery.

6 **B.3. THE COMMISSION OF ACTS PROHIBITED BY THE ANTI-**
7 **TRAFFICKING IN PERSONS ACT OF 2003, AS AMENDED, THROUGH**
8 **OR USING DEVICES, EQUIPMENT, OR PHYSICAL PLANTS**
9 **CONNECTED TO THE INTERNET OR TO TELECOMMUNICATIONS**
10 **NETWORKS SHALL BE PENALIZED BY THE APPLICABLE**
11 **PROVISIONS OF THE ANTI-TRAFFICKING IN PERSONS ACT OF**
12 **2003, AS AMENDED.**

13 *Section 32. ICT-Enabled Child Prostitution and ICT-Enabled Child Trafficking. –*

14 A.1. *ICT-Enabled Child Prostitution.* - The performance of acts prohibited by Sections 5
15 and 7 of R.A. No. 7610, or the “Special Protection of Children Against Abuse, Exploitation and
16 Discrimination Act,” as amended, by means of a device, storage medium, network equipment, or
17 physical plant connected to the Internet or to telecommunications networks shall be deemed
18 unlawful.

19 A.2. Section 5 of the “Special Protection of Children Against Abuse, Exploitation and
20 Discrimination Act” shall be amended to read:

21 Section 5. *Child Prostitution and Other Sexual Abuse.* – Children, whether
22 male or female, who for money, profit, or any other consideration or due to the
23 coercion or influence of any adult, syndicate or group, indulge in sexual
24 intercourse or lascivious conduct, are deemed to be children exploited in
25 prostitution and other sexual abuse.

26 The penalty of *reclusion temporal* in its medium period to *reclusion*
27 *perpetua* shall be imposed upon the following:

1 (a) Those who engage in or promote, facilitate or induce child prostitution
2 which include, but are not limited to, the following:

3 (1) Acting as a procurer of a child prostitute;

4 (2) Inducing a person to be a client of a child prostitute by means
5 of written or oral advertisements or other similar means; **OR TO**
6 **KNOWINGLY, WILLFULLY AND INTENTIONALLY PROVIDE**
7 **DEVICES, EQUIPMENT, OR PHYSICAL PLANTS CONNECTED**
8 **TO THE INTERNET OR TO TELECOMMUNICATIONS**
9 **NETWORKS WITH THE PRIMARY PURPOSE OF INDUCING A**
10 **PERSON TO BE A CLIENT OF A CHILD PROSTITUTE OR**
11 **THROUGH THE CONNIVANCE WITH A THIRD PARTY WITH**
12 **ACCESS TO THE SAME INDUCE A PERSON TO BE A CLIENT**
13 **OF A CHILD PROSTITUTE;**

14 (3) Taking advantage of influence or relationship to procure a child
15 as prostitute;

16 (4) Threatening or using violence towards a child to engage him as
17 a prostitute; or

18 (5) Giving monetary consideration goods or other pecuniary
19 benefit to a child with intent to engage such child in prostitution.

20 (b) Those who commit the act of sexual intercourse or lascivious conduct
21 with a child exploited in prostitution or subject to other sexual abuse; Provided,
22 That when the victims is under twelve (12) years of age, the perpetrators shall be
23 prosecuted under Article 335, paragraph 3, for rape and Article 336 of Act No.
24 3815, as amended, the Revised Penal Code, for rape or lascivious conduct, as the
25 case may be: Provided, That the penalty for lascivious conduct when the victim is
26 under twelve (12) years of age shall be *reclusion temporal* in its medium period;
27 and

28 (c) Those who derive profit or advantage therefrom, whether as manager
29 or owner of the establishment where the prostitution takes place, or of the sauna,

1 disco, bar, resort, place of entertainment or establishment serving as a cover or
2 which engages in prostitution in addition to the activity for which the license has
3 been issued to said establishment; **OR THOSE WHO DERIVE PROFIT OR**
4 **ADVANTAGE THEREFROM, WHETHER AS AUTHOR,**
5 **ADMINISTRATOR, OR AUTHORIZED USER OF THE DEVICE,**
6 **EQUIPMENT, NETWORK, PHYSICAL PLANT, OR WEBSITE**
7 **CONNECTED TO THE INTERNET OR TO TELECOMMUNICATIONS**
8 **NETWORKS CREATED OR ESTABLISHED WITH THE PURPOSE OF**
9 **INDUCING A PERSON TO ENGAGE IN CHILD PROSTITUTION.**

10 B.1. *ICT-Enabled Child Trafficking.* – Section 7 of the “Special Protection of Children
11 Against Abuse, Exploitation and Discrimination Act” shall be amended to read:

12 Section 7. *Child Trafficking.* – Any person who shall engage in trading
13 and dealing with children including, but not limited to, the act of buying and
14 selling of a child for money, or for any other consideration, or barter, **OR TO**
15 **KNOWINGLY, WILLFULLY AND INTENTIONALLY PROVIDE**
16 **DEVICES, EQUIPMENT, OR PHYSICAL PLANTS CONNECTED TO**
17 **THE INTERNET OR TO TELECOMMUNICATIONS NETWORKS, OR**
18 **THROUGH THE CONNIVANCE WITH A THIRD PARTY WITH**
19 **ACCESS TO THE SAME, FOR THE PRIMARY PURPOSE OF SUCH**
20 **TRADING AND DEALING WITH CHILDREN,** shall suffer the penalty of
21 *reclusion temporal to reclusion perpetua.* The penalty shall be imposed in its
22 maximum period when the victim is under twelve (12) years of age.

23 B.2. The commission of acts prohibited by the “Special Protection of Children Against
24 Abuse, Exploitation and Discrimination Act,” as amended, through or using devices, equipment,
25 or physical plants connected to the Internet or to telecommunications networks shall be penalized
26 by the applicable provisions of the “Special Protection of Children Against Abuse, Exploitation
27 and Discrimination Act,” as amended.

1 Section 33. *Internet Libel, Hate Speech, Child Pornography, and Other Expression*
2 *Inimical to the Public Interest.* –

3 A.1. *Internet libel.* – Internet libel is a public and malicious expression tending to cause
4 the dishonor, discredit, or contempt of a natural or juridical person, or to blacken the memory of
5 one who is dead, made on the Internet or on public networks.

6 A.2. *Malice as an essential element of internet libel.* – Internet libel shall not lie if malice
7 or intent to injure is not present.

8 A.3. *Positive identification of the subject as an essential element of internet libel.* –
9 Internet libel shall not lie if the public and malicious expression does not explicitly identify the
10 person who is the subject of the expression, except if the content of the expression is sufficient
11 for positive and unequivocal identification of the subject of the expression.

12 A.4. *Exceptions to internet libel.* – The following acts shall not constitute internet libel:

13 a) Expressions of protest against the government, or against foreign governments;

14 b) Expressions of dissatisfaction with the government, its agencies or instrumentalities, or
15 its officials or agents, or with those of foreign governments;

16 c) Expressions of dissatisfaction with non-government organizations, unions,
17 associations, political parties, religious groups, and public figures;

18 d) Expressions of dissatisfaction with the products or services of commercial entities;

19 e) Expressions of dissatisfaction with commercial entities, or their officers or agents, as
20 related to the products or services that the commercial entities provide;

21 f) Expressions of a commercial entity that are designed to discredit the products or
22 services of a competitor, even if the competitor is explicitly identified;

23 g) An expression made with the intention of remaining private between persons able to
24 access or view the expression, even if the expression is later released to the public; and,

25 h) A fair and true report, made in good faith, without any comments or remarks, of any
26 judicial, legislative or other official proceedings, or of any statement, report or speech delivered
27 in said proceedings, or of any other act performed by public officers in the exercise of their
28 functions, or of any matter of public interest.

1 A.5. *Truth as a defense.* – Internet libel shall not lie if the content of the expression is
2 proven to be true, or if the expression is made on the basis of published reports presumed to be
3 true, or if the content is intended to be humorous or satirical in nature, except if the content has
4 been adjudged as unlawful or offensive in nature in accordance with existing jurisprudence.

5 B.1. *Internet hate speech.* – Internet hate speech is a public and malicious expression
6 calling for the commission of illegal acts on an entire class of persons, a reasonably broad
7 section thereof, or a person belonging to such a class, based on gender, sexual orientation,
8 religious belief or affiliation, political belief or affiliation, ethnic or regional affiliation,
9 citizenship, or nationality, made on the Internet or on public networks.

10 B.2. *Call for the commission of illegal acts as an essential element for internet hate*
11 *speech.* – Internet hate speech shall not lie if the expression does not call for the commission of
12 illegal acts on the person or class of persons that, when they are done, shall cause actual criminal
13 harm to the person or class of persons, under existing law.

14 B.3. *Imminent lawless danger as an essential element for internet hate speech.* – Internet
15 hate speech shall not lie if the expression does not call for the commission of illegal acts posing
16 an immediate lawless danger to the public or to the person who is the object of the expression.

17 C.1. *Internet child pornography.* – The performance of acts prohibited by Sections 4 and
18 5 of R.A. No. 9775, or the “Anti-Child Pornography Act of 2009,” as amended, by means of a
19 device, storage medium, network equipment, or physical plant connected to the Internet or to
20 telecommunications networks shall be deemed unlawful.

21 C.2. Sections 4 (e) and (f) of the Anti-Child Pornography Act of 2009 shall be amended
22 to read:

23 (e) To knowingly, willfully and intentionally provide a venue for the
24 commission of prohibited acts as, but not limited to, dens, private rooms, cubicles,
25 cinemas, houses or in establishments purporting to be a legitimate business; **OR**
26 **TO KNOWINGLY, WILLFULLY AND INTENTIONALLY PROVIDE**
27 **DEVICES, EQUIPMENT, OR PHYSICAL PLANTS CONNECTED TO**
28 **THE INTERNET OR TO TELECOMMUNICATIONS NETWORKS FOR**

1 **THE PRIMARY PURPOSE OF PUBLICATION, OFFERING,**
2 **PRODUCTION, SELLING, DISTRIBUTION, BROADCASTING,**
3 **EXPORT, OR IMPORTATION OF CHILD PORNOGRAPHY;**

4 (f) For film distributors, theaters, **INTERNET SERVICE PROVIDERS,**
5 and telecommunication companies, by themselves or in cooperation with other
6 entities, to distribute any form of child pornography;

7 C.3. The commission of acts prohibited by the Anti-Child Pornography Act of 2009, as
8 amended, through or using devices, equipment, or physical plants connected to the Internet or to
9 telecommunications networks shall be penalized by the applicable provisions of the Anti-Child
10 Pornography Act of 2009, as amended.

11 C.4. *Internet child abuse.* – The performance of acts prohibited by Section 9 of the
12 Special Protection of Children Against Abuse, Exploitation and Discrimination Act, as amended,
13 by means of a device, storage medium, network equipment, or physical plant connected to the
14 Internet or to telecommunications networks shall be deemed unlawful.

15 C.5. Section 9 of the Special Protection of Children Against Abuse, Exploitation and
16 Discrimination Act shall be amended to read:

17 Section 9. *Obscene Publications and Indecent Shows.* – Any person who
18 shall hire, employ, use, persuade, induce or coerce a child to perform in obscene
19 exhibitions and indecent shows, whether live, in video, or through the Internet or
20 telecommunications networks, or model in obscene publications or pornographic
21 materials or to sell or distribute or **CAUSE THE PUBLICATION IN THE**
22 **INTERNET OR THROUGH TELECOMMUNICATIONS NETWORKS** the
23 said materials shall suffer the penalty of *prision mayor* in its medium period.

24 If the child used as a performer, subject or seller/distributor is below
25 twelve (12) years of age, the penalty shall be imposed in its maximum period.

26 Any ascendant, guardian, or person entrusted in any capacity with the care
27 of a child who shall cause and/or allow such child to be employed or to participate
28 in an obscene play, scene, act, movie or show or in any other acts covered by this
29 section shall suffer the penalty of *prision mayor* in its medium period.

1 C.6. The commission of acts prohibited by the Special Protection of Children Against
2 Abuse, Exploitation and Discrimination Act, as amended, through or using devices, equipment,
3 or physical plants connected to the Internet or to telecommunications networks shall be penalized
4 by the applicable provisions of the Special Protection of Children Against Abuse, Exploitation
5 and Discrimination Act, as amended.

6 D.1. *Expression inimical to the public interest.* – Except upon a final ruling from the
7 courts, issued following due notice or hearing, no expression made on the Internet or on public
8 networks that is not defined in this section shall be deemed unlawful and inimical to the public
9 interest.

10 D.2. *Imminent lawless danger as an essential element of expression inimical to public*
11 *interest.* – No expression shall be deemed inimical to the public interest if the expression does
12 not call for the commission of illegal acts posing an immediate lawless danger to the public.

13 *Section 34. Sabotage of critical networks and infrastructure, and other acts of*
14 *cyberterrorism.* –

15 A. 1. *Sabotage of critical networks and infrastructure.* – The commission of acts
16 prohibited by Section 24 (Network Sabotage), Section 26 (Violation of Data Privacy), Section 27
17 (Violation of Data Security), and Section 28 (Illegal and Arbitrary Seizure of ICT), shall be
18 penalized one degree higher; Provided, the offense was committed against critical data, network,
19 Internet, or telecommunications infrastructure, whether publicly or privately owned.

20 B.1. *Cyberterrorism.* – The performance of acts prohibited by Sections 3, 4, 5, and 6 of
21 R.A. No. 9732, or the “Human Security Act of 2007,” as amended, and Sections 4, 5, 6, and 7 of
22 R.A. No. 10168, or the “Terrorism Financing Prevention and Suppression Act of 2012,” by
23 means of a device, storage medium, network equipment, or physical plant connected to the
24 Internet or to telecommunications networks shall be deemed unlawful.

25 B.2. Section 3 of the Human Security Act of 2007 shall be amended to read:

26 Section. 3. *Terrorism.* – Any person who commits an act punishable under
27 any of the following provisions of the Revised Penal Code:

1 1. Article 122 (Piracy in General and Mutiny in the High Seas or in the
2 Philippine Waters);

3 2. Article 134 (Rebellion or Insurrection);

4 3. Article 134-a (Coup d' Etat), including acts committed by private
5 persons;

6 4. Article 248 (Murder);

7 5. Article 267 (Kidnapping and Serious Illegal Detention);

8 6. Article 324 (Crimes Involving Destruction),

9 or under

10 1. Presidential Decree No. 1613 (The Law on Arson);

11 2. Republic Act No. 6969 (Toxic Substances and Hazardous and Nuclear
12 Waste Control Act of 1990);

13 3. Republic Act No. 5207 (Atomic Energy Regulatory and Liability Act of
14 1968);

15 4. Republic Act No. 6235 (Anti-Hijacking Law);

16 5. Presidential Decree No. 532 (Anti-Piracy and Anti-Highway Robbery
17 Law of 1974);

18 6. Presidential Decree No. 1866, as amended (Decree Codifying the Laws
19 on Illegal and Unlawful Possession, Manufacture, Dealing in, Acquisition or
20 Disposition of Firearms, Ammunitions or Explosives); and,

21 **7. SECTION 25 (NETWORK SABOTAGE), SECTION 27**
22 **(VIOLATION OF DATA PRIVACY), AND SECTION 28 (VIOLATION OF**
23 **DATA SECURITY) OF THE MAGNA CARTA FOR PHILIPPINE**
24 **INTERNET FREEDOM COMMITTED AGAINST CRITICAL DATA,**
25 **NETWORK, INTERNET, OR TELECOMMUNICATIONS**
26 **INFRASTRUCTURE, WHETHER PUBLICLY OR PRIVATELY OWNED,**

27 thereby sowing and creating a condition of widespread and extraordinary fear and
28 panic among the populace, in order to coerce the government to give in to an
29

1 unlawful demand shall be guilty of the crime of terrorism and shall suffer the
2 penalty of forty (40) years of imprisonment, without the benefit of parole as
3 provided for under Act No. 4103, otherwise known as the Indeterminate Sentence
4 Law, as amended.

5 B.3. The commission of acts prohibited by the Human Security Act of 2007, as amended,
6 through or using devices, equipment, or physical plants connected to the Internet or to
7 telecommunications networks shall be penalized by the applicable provisions of the Human
8 Security Act of 2007, as amended.

9 C.1. *ICT-Enabled Financing of Terrorism.* – Section 4 of the Terrorism Financing
10 Prevention and Suppression Act of 2012 shall be amended to read:

11 Section 4. *Financing of Terrorism.* – Any person who, directly or
12 indirectly, willfully and without lawful excuse, possesses, provides, collects or
13 uses property or funds or makes available property, funds or financial service or
14 other related services, by any means, with the unlawful and willful intention that
15 they should be used or with the knowledge that they are to be used, in full or in
16 part: (a) to carry out or facilitate the commission of any terrorist act; (b) by a
17 terrorist organization, association or group; or (c) by an individual terrorist, shall
18 be guilty of the crime of financing of terrorism and shall suffer the penalty of
19 *reclusion temporal* in its maximum period to *reclusion perpetua* and a fine of not
20 less than Five hundred thousand pesos (Php500,000.00) nor more than One
21 million pesos (Php1,000,000.00).

22 Any person who organizes or directs others to commit financing of
23 terrorism under the immediately preceding paragraph shall likewise be guilty of
24 an offense and shall suffer the same penalty as herein prescribed.

25 **ANY PERSON WHO, BY MEANS OF A DEVICE, STORAGE**
26 **MEDIUM, NETWORK EQUIPMENT, OR PHYSICAL PLANT**
27 **CONNECTED TO THE INTERNET OR TO TELECOMMUNICATIONS**
28 **NETWORKS, OR IN CONNIVANCE WITH A THIRD PARTY WITH**

1 ACCESS TO THE SAME, SHALL KNOWINGLY, WILLFULLY, AND
2 INTENTIONALLY FACILITATE THE ORGANIZATION OR
3 DIRECTION OF OTHERS TO COMMIT THE FINANCING OF
4 TERRORISM UNDER THE PRECEDING PARAGRAPHS SHALL
5 LIKEWISE BE GUILTY OF AN OFFENSE AND SHALL SUFFER THE
6 SAME PENALTY AS HEREIN PRESCRIBED.

7 For purposes of this Act, knowledge or intent may be established by direct
8 evidence or inferred from the attendant circumstances.

9 For an act to constitute a crime under this Act, it shall not be necessary
10 that the funds were actually used to carry out a crime referred to in Section 3(j).

11 C.2. The commission of acts prohibited by the Terrorism Financing Prevention and
12 Suppression Act of 2012, as amended, through or using devices, equipment, or physical plants
13 connected to the Internet or to telecommunications networks shall be penalized by the applicable
14 provisions of the Terrorism Financing Prevention and Suppression Act of 2012, as amended.

15 Chapter VIII. Penalties.

16 *Section 35. Applicability of the Revised Penal Code and other special laws. –*
17 Nomenclature notwithstanding, the provisions of Book I of the Revised Penal Code shall apply
18 suppletorily to the provisions of this Act, whenever applicable.

19 The provisions of special laws shall apply as provided for by this Act.

20 *Section 36. Penalties For Specific Violations of The Magna Carta for Philippine Internet*
21 *Freedom. –* The following penalties shall be imposed for specific violations of this Act:

22 1. Violation of Section 24. A. (Direct network sabotage) – Shall be punished with
23 imprisonment of *prision correccional* or a fine of not more than Five hundred thousand pesos
24 (PhP500,000.00) or both.

25 2. Violation of Section 24. B. (Indirect network sabotage) - Shall be punished with
26 imprisonment of *prision correccional* in its medium period or a fine of not more than three
27 hundred thousand pesos (PhP300,000.00) or both.

1 3. Violation of Section 25. A. (Failure to provide security) - Shall be punished with
2 imprisonment of *prision correccional* or a fine of not more than Five hundred thousand pesos
3 (PhP500,000.00) or both.

4 4. Violation of Section 25. B. (Negligent failure to provide security) - Shall be punished
5 with imprisonment of *prision correccional* or a fine of not more than Five hundred thousand
6 pesos (PhP500,000.00) or both.

7 5. Violation of Section 26. A. (Unauthorized access) – Shall be punished with
8 imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five
9 hundred thousand pesos (Php500,000.00) but not more than Two million pesos
10 (Php2,000,000.00).

11 6. Violation of Section 26. B. (Unauthorized modification) - Shall be punished with
12 imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five
13 hundred thousand pesos (Php500,000.00) but not more than Two million pesos
14 (Php2,000,000.00).

15 7. Violation of Section 26. C. (Unauthorized granting of privileges) - Shall be punished
16 with imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five
17 hundred thousand pesos (Php500,000.00) but not more than Two million pesos
18 (Php2,000,000.00).

19 8. Violation of Section 26. D. (Unauthorized disclosure) - imprisonment ranging from
20 three (3) years to five (5) years and a fine of not less than Five hundred thousand pesos
21 (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

22 9. Violations of the Section 26. E. (Violation of Data Privacy Act through ICT) –

23 9.1. Violation of Section 25 (a) of the Data Privacy Act (Unauthorized Processing
24 of Personal Information) through ICT – imprisonment ranging from one (1) year to three
25 (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not
26 more than Two million pesos (Php2,000,000.00).

27 9.2. Violation of Section 25 (b) of the Data Privacy Act (Unauthorized Processing
28 of Sensitive Personal Information) through ICT – imprisonment ranging from three (3)

1 years to six (6) years and a fine of not less than Five hundred thousand pesos
2 (Php500,000.00) but not more than Four million pesos (Php4,000,000.00).

3 9.3. Violation of Section 26 (a) of the Data Privacy Act (Accessing Personal
4 Information Due to Negligence) through ICT – imprisonment ranging from one (1) year
5 to three (3) years and a fine of not less than Five hundred thousand pesos
6 (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

7 9.4. Violation of Section 26 (b) of the Data Privacy Act (Accessing Sensitive
8 Personal Information Due to Negligence) through ICT – imprisonment ranging from
9 three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos
10 (Php500,000.00) but not more than Four million pesos (Php4,000,000.00).

11 9.5. Violation of Section 27 (a) of the Data Privacy Act (Improper Disposal of
12 Personal Information) through ICT – imprisonment ranging from six (6) months to two
13 (2) years and a fine of not less than One hundred thousand pesos (Php100,000.00) but not
14 more than Five hundred thousand pesos (Php500,000.00).

15 9.6. Violation of Section 27 (b) of the Data Privacy Act (Improper Disposal of
16 Sensitive Personal Information) through ICT – imprisonment ranging from one (1) year
17 to three (3) years and a fine of not less than One hundred thousand pesos
18 (Php100,000.00) but not more than One million pesos (Php1,000,000.00).

19 9.7. Violation of Section 28 (a) of the Data Privacy Act (Processing of Personal
20 Information for Unauthorized Purposes) through ICT – imprisonment ranging from one
21 (1) year and six (6) months to five (5) years and a fine of not less than Five hundred
22 thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

23 9.8. Violation of Section 28 (b) of the Data Privacy Act (Processing of Sensitive
24 Personal Information for Unauthorized Purposes) through ICT – imprisonment ranging
25 from two (2) years to seven (7) years and a fine of not less than Five hundred thousand
26 pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

27 9.9. Violation of Section 30 of the Data Privacy Act (Concealment of Security
28 Breaches Involving Sensitive Personal Information) through ICT – imprisonment of one

1 (1) year and six (6) months to five (5) years and a fine of not less than Five hundred
2 thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

3 9.10. Violation of Section 33 of the Data Privacy Act (Combination or Series of
4 Acts) through ICT – imprisonment ranging from three (3) years to six (6) years and a fine
5 of not less than One million pesos (Php1,000,000.00) but not more than Five million
6 pesos (Php5,000,000.00).

7 10. Violation of Section 27. A. (Hacking) – imprisonment ranging from one (1) year to
8 three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not
9 more than Two million pesos (Php2,000,000.00).

10 11. Violation of Section 27. B. (Cracking) – imprisonment ranging from one (1) year to
11 three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not
12 more than Two million pesos (Php2,000,000.00).

13 12. Violation of Section 27. C. (Phishing) – imprisonment ranging from one (1) year and
14 six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos
15 (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

16 13. Violation of Section 27. D. (Violation of Data Privacy Act with hacking, cracking, or
17 phishing)

18 13.1. Violation of Section 25 (a) of the Data Privacy Act (Unauthorized
19 Processing of Personal Information) with hacking, cracking, or phishing – shall be
20 penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not
21 less than Five hundred thousand pesos (Php500,000.00) but not more than Two million
22 pesos (Php2,000,000.00).

23 13.2. Violation of Section 25 (b) of the Data Privacy Act (Unauthorized
24 Processing of Sensitive Personal Information) with hacking, cracking, or phishing – shall
25 be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of
26 not less than Five hundred thousand pesos (Php500,000.00) but not more than Four
27 million pesos (Php4,000,000.00).

28 13.3. Violation of Section 26 (a) of the Data Privacy Act (Accessing Personal
29 Information Due to Negligence) with hacking, cracking, or phishing – shall be penalized

1 by imprisonment ranging from one (1) year to three (3) years and a fine of not less than
2 Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos
3 (Php2,000,000.00).

4 13.4. Violation of Section 26 (b) of the Data Privacy Act (Accessing Sensitive
5 Personal Information Due to Negligence) with hacking, cracking, or phishing – shall be
6 penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not
7 less than Five hundred thousand pesos (Php500,000.00) but not more than Four million
8 pesos (Php4,000,000.00).

9 13.5. Violation of Section 27 (a) of the Data Privacy Act (Improper Disposal of
10 Personal Information) with hacking, cracking, or phishing – shall be penalized by
11 imprisonment ranging from six (6) months to two (2) years and a fine of not less than
12 One hundred thousand pesos (Php100,000.00) but not more than Five hundred thousand
13 pesos (Php500,000.00).

14 13.6. Violation of Section 27 (b) of the Data Privacy Act (Improper Disposal of
15 Sensitive Personal Information) with hacking, cracking, or phishing – shall be penalized
16 by imprisonment ranging from one (1) year to three (3) years and a fine of not less than
17 One hundred thousand pesos (Php100,000.00) but not more than One million pesos
18 (Php1,000,000.00).

19 13.7. Violation of Section 28 (a) of the Data Privacy Act (Processing of Personal
20 Information for Unauthorized Purposes) with hacking, cracking, or phishing – shall be
21 penalized by imprisonment ranging from one (1) year and six (6) months to five (5) years
22 and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more
23 than One million pesos (Php1,000,000.00).

24 13.8. Violation of Section 28 (b) of the Data Privacy Act (Processing of Sensitive
25 Personal Information for Unauthorized Purposes) with hacking, cracking, or phishing –
26 shall be penalized by imprisonment ranging from two (2) years to seven (7) years and a
27 fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than
28 Two million pesos (Php2,000,000.00).

1 13.9. Violation of Section 30 of the Data Privacy Act (Concealment of Security
2 Breaches Involving Sensitive Personal Information) with hacking, cracking, or phishing –
3 Shall be penalized by imprisonment of one (1) year and six (6) months to five (5) years
4 and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more
5 than One million pesos (Php1,000,000.00).

6 13.10. Violation of Section 33 of the Data Privacy Act (Combination or Series of
7 Acts) with hacking, cracking, or phishing – shall be penalized by imprisonment ranging
8 from three (3) years to six (6) years and a fine of not less than One million pesos
9 (Php1,000,000.00) but not more than Five million pesos (Php5,000,000.00).

10 14. Violation of Section 28. A. (Illegal seizure of ICT) – shall be punished with
11 imprisonment of *prision correccional* or a fine of not more than Five hundred thousand pesos
12 (PhP500,000.00) or both.

13 15. Violation of Section 28. B. (Aiding and abetting illegal seizure of ICT) – shall be
14 punished with imprisonment of *prision correccional* in its minimum period or a fine of not more
15 than Four hundred thousand pesos (PhP400,000.00) or both.

16 16. Violation of Section 28. C. (Arbitrary seizure of ICT) – Shall be punished with
17 imprisonment of *prision correccional* in its maximum period or a fine of not more than Five
18 hundred thousand pesos (PhP500,000.00) or both.

19 17. Violation of Section 28. D. (Instigating arbitrary seizure of ICT) – shall be punished
20 with imprisonment of *prision correccional* or a fine of not more than Five hundred thousand
21 pesos (PhP500,000.00) or both.

22 18. Violation of Section 29. A. 1. (Copyright infringement) – any person infringing a
23 copyright shall be liable to pay to the copyright proprietor or his assigns or heirs such actual
24 damages, including legal costs and other expenses, as he may have incurred due to the
25 infringement as well as the profits the infringer may have made due to such infringement, and in
26 proving profits the plaintiff shall be required to prove sales only and the defendant shall be
27 required to prove every element of cost which he claims, or, in lieu of actual damages and
28 profits, such damages which to the court shall appear to be just and shall not be regarded as
29 penalty.

1 19. Violation of Section 29. A. 2. (Plagiarism of copyleft) – The same penalty for a
2 violation of Section 29. A. 1. (Copyright infringement) shall be imposed for a violation of this
3 Section.

4 20. Violation of Section 29. A. 3. (Plagiarism of public domain content) – While this
5 constitutes infringement, it shall not be subject to the payment of damages or to any other
6 penalty.

7 21. Violation of Section 29. A. 4. (Reverse engineering) – The same penalty for a
8 violation of Section 29. A. 1. (Copyright infringement) shall be imposed for a violation of this
9 Section.

10 22. Violation of Section 29. B. 1. (Piracy through ICT) – The same penalty for a violation
11 of Section 29. A. 1. (Copyright infringement) shall be imposed for a violation of this Section.

12 23. Violation of Section 29. C. 1. (Cybersquatting) – The same penalty for a violation of
13 Section 29. A. 1. (Copyright infringement) shall be imposed for a violation of this Section.

14 24. Violation of Section 29. D. 1. (Unreasonable restriction of device privileges) – shall
15 be punished with a fine of not less than one hundred thousand pesos (PhP 100,000.00) or more
16 than two million pesos (PhP 2,000,000.00).

17 25. Violation of Section 30. A. 1. (Fraud via ICT) – shall be punished with imprisonment
18 of *prision correccional* or a fine of at least Two hundred thousand pesos (PhP200,000.00) up to a
19 maximum amount that is double the amount of damage incurred, whichever is higher, or both
20 imprisonment and fine.

21 26. Violation of Section 31. A. 1. (ICT-enabled prostitution) – shall be punished with
22 imprisonment of *prision mayor* or a fine of at least Two hundred thousand pesos
23 (PhP200,000.00) up to a maximum amount of Five hundred thousand pesos (PhP500,000.00), or
24 both.

25 27. Violation of Section 31. B. 1. (ICT-enabled trafficking in persons)

26 27.1. Violation of Section 4 of the Anti-Trafficking in Persons Act of 2003
27 through ICT – penalty of imprisonment of twenty (20) years and a fine of not less than
28 One million pesos (P1,000,000.00) but not more than Two million pesos (P2,000,000.00).

1 27.2. Violation of Section 5 of the Anti-Trafficking in Persons Act of 2003
2 through ICT – imprisonment of fifteen (15) years and a fine of not less than Five hundred
3 thousand pesos (P500,000.00) but not more than One million pesos (P1,000,000.00).

4 27.3. Violation of Section 6 of the Anti-Trafficking in Persons Act of 2003
5 through ICT – life imprisonment and a fine of not less than Two million pesos
6 (P2,000,000.00) but not more than Five million pesos (P5,000,000.00).

7 27.4. Violation of Section 7 of the Anti-Trafficking in Persons Act of 2003
8 through ICT – imprisonment of six (6) years and a fine of not less than Five hundred
9 thousand pesos (P500,000.00) but not more than One million pesos (P1,000,000.00).

10 28. Violation of Section 32. A. 1. (ICT-enabled child prostitution)

11 28.1. Violation of Section 5 of the Special Protection of Children Against Abuse,
12 Exploitation and Discrimination Act through ICT – *reclusion temporal* in its medium
13 period to *reclusion perpetua*.

14 29. Violation of Section 32. B. 1. (ICT-enabled child trafficking)

15 29.1. Violation of Section 7 of the Special Protection of Children Against Abuse,
16 Exploitation and Discrimination Act through ICT – *reclusion temporal* to *reclusion*
17 *perpetua*. The penalty shall be imposed in its maximum period when the victim is under
18 twelve (12) years of age.

19 30. Violation of Section 33. A. 1. (Internet libel) – This shall only give rise to civil
20 liability and the amount shall be commensurate to the damages suffered.

21 31. Violation of Section 33. B. 1. (Internet hate speech) – This shall only give rise to civil
22 liability and the amount shall be commensurate to the damages suffered.

23 32. Violation of Section 33. C. 1. (Internet child pornography)

24 32.1. Violation of the Anti-Child Pornography Act through ICT – Shall be punished
25 according to the provisions of Section 15 of R.A. No. 9775, or the “Anti-Child Pornography Act
26 of 2009.”

27 33. Violation of Section 33. C. 4. (Internet child abuse)

28 33.1. Violation of Section 9 of the Special Protection of Children Against Abuse,
29 Exploitation and Discrimination Act through ICT - Shall be punished with imprisonment

1 of *prision mayor* in its medium period. If the child used as a performer, subject or seller/
2 distributor is below twelve (12) years of age, the penalty shall be imposed in its
3 maximum period.

4 34. Violation of Section 33. D. 1. (Internet expression inimical to the public interest) –
5 This shall only give rise to civil liability and the amount shall be commensurate to the damages
6 caused by the Internet expression.

7 35. Violation of Section 34. B. 1. (Cyberterrorism) – The commission of acts prohibited
8 by the Human Security Act of 2007, as amended, through or using devices, equipment, or
9 physical plants connected to the Internet or to telecommunications networks shall be penalized
10 by the applicable provisions of the Human Security Act of 2007, as amended.

11 36. Violation of Section 34. C. 1. (ICT-enabled financing of terrorism) – The commission
12 of acts prohibited by the Terrorism Financing Prevention and Suppression Act of 2012, as
13 amended, through or using devices, equipment, or physical plants connected to the Internet or to
14 telecommunications networks shall be penalized by the applicable provisions of the Terrorism
15 Financing Prevention and Suppression Act of 2012, as amended.

16 *Section 37. Penalties for Violations of the Magna Carta for Philippine Internet Freedom*
17 *Affecting Critical Networks and Infrastructure.* – As prescribed by Section 34. A. 1. of this Act,
18 a penalty one degree higher shall be imposed on the specific violations of the Magna Carta for
19 Philippine Internet Freedom if committed against critical networks or information and
20 communications technology infrastructure.

21 *Section 38. Penalties for Other Violations of The Magna Carta for Philippine Internet*
22 *Freedom.* – A fine of not more than Five hundred thousand pesos (PhP 500,000.00) shall be
23 imposed for a violation of other sections of the law not covered by the preceding sections.

24 *Section 39. Penalties for Violations of The Magna Carta for Philippine Internet Freedom*
25 *Committed by a Public Official or Employee.* –

26 1. Except as explicitly provided by the preceding sections, the next higher penalty shall
27 be imposed for a violation or negligence resulting in the violation of this Act if the violation or

1 negligence resulting in the violation is committed by a public official or employee in connection
2 with his duties.

3 2. If the penalty imposed for the act or negligence resulting in the violation of this Act is
4 civil liability or civil liability and a fine, then an additional penalty of a fine of not less Two
5 hundred thousand pesos (PhP 200,000.00) but not more than Five hundred thousand pesos (PhP
6 500,000.00) shall be imposed on the public official or employee.

7 *Section 40. Liability Under the Data Privacy Act, the Intellectual Property Code, the*
8 *Optical Media Act, the Anti-Child Pornography Act of 2009, the Special Protection of Children*
9 *Against Abuse, Exploitation and Discrimination Act, the Revised Penal Code, and Other Laws. --*

10 1. A prosecution under this act shall bar any further prosecution of the act as a violation
11 of any provision of the Data Privacy Act, the Intellectual Property Code, the Optical Media Act,
12 the Anti-Child Pornography Act of 2009, the Anti-Trafficking in Persons Act, and other special
13 laws, except: a) if the act was performed through the use of a device, equipment, or physical
14 plant connected to the Internet or to telecommunications networks, or in connivance with a third
15 party with access to the same; b) if the act could not have been performed through the use the
16 said device, equipment, or physical plant connected to the Internet or to telecommunications
17 networks, or the said third party with access to the same, and; c) if the act is part of a series of or
18 combination with other unlawful acts, these acts being performed without the use of a device,
19 equipment, or physical plant connected to the Internet or to telecommunications networks, or in
20 connivance with a third party with access to the same.

21 2. A prosecution under this act shall bar any further prosecution of the act as a violation
22 of the Revised Penal Code and other special laws, except: a) if the act was performed through the
23 use of a device, equipment, or physical plant connected to the Internet or to telecommunications
24 networks, or in connivance with a third party with access to the same; b) if the violation could
25 not have been performed through the use the said device, equipment, or physical plant connected
26 to the Internet or to telecommunications networks, or the said third party with access to the same;
27 c) if the act involves the transmission of data through the Internet or telecommunications
28 networks, and d) if the act is part of a series of or combination with other unlawful acts, these

1 acts being performed without the use of a device, equipment, or physical plant connected to the
2 Internet or to telecommunications networks, or in connivance with a third party with access to
3 the same.

4 **Chapter IX. Cybercrime Law Enforcement and Jurisdiction.**

5 *Section 41. Competent law enforcement agencies. –*

6 1. *Department of Justice (DOJ).* – There is hereby created an Office of Cybercrime
7 within the DOJ, which shall be designated as the central authority in the enforcement of this Act,
8 and all matters related to international mutual assistance and extradition, as provided for by this
9 Act.

10 2. *National Bureau of Investigation (NBI).* – There is hereby created a separate
11 Cybercrime Division within the NBI, which shall be responsible for matters related to
12 enforcement of this Act. It shall cooperate with the division responsible for matters related with
13 transnational crime, other divisions, and other government agencies in the enforcement of this
14 Act.

15 3. *Philippine National Police (PNP).* – There is hereby created a separate Cybercrime
16 Office attached to the Criminal Investigation and Detection Group (CIDG), which shall be
17 responsible for matters related to enforcement of this Act. The PNP shall establish cybercrime
18 desks in police stations, and shall cooperate with other government agencies in the enforcement
19 of this Act.

20 *Section 42. Cybercrime courts. –*

21 1. *Cybercrime courts.* – Cybercrime courts, manned by judges of competence, integrity,
22 probity and independence in the practice of law, and competent in matters related to the Internet
23 and information and communications technology, shall be established at every city and
24 provincial capital in the country.

25 2. *Qualifications of the Presiding Judges of cybercrime courts.* – No person shall be
26 appointed a Presiding Judge of the Cybercrime Court unless he:

27 a) is a natural-born citizen of the Philippines;

1 b) is at least thirty-five (35) years of age;

2 c) has been engaged in the practice of law in the Philippines for at least ten (10)
3 years, or has held a public office in the Philippines requiring admission to the practice of
4 law as an indispensable requisite; and,

5 d) has an academic or professional background in information and
6 communications technology, computer science, or engineering; or has proven a high
7 degree of competence in the use of the Internet and information and communications
8 technology.

9 Court personnel of the Cybercrime Court shall undergo training and must have the
10 experience and demonstrated ability in dealing with cybercrime cases and other cases
11 related to the Internet and information and communications technology.

12 3. *Mandatory continuing legal and information and communications technology*
13 *education.* – The Supreme Court shall provide a continuing education program on the Internet,
14 information and communications technology, cybercrime law, procedure, and other related
15 disciplines to judges and personnel of cybercrime courts.

16 4. *Special rules of procedure for cybercrime courts.* – The Supreme Court shall
17 promulgate special rules of procedure for cybercrime courts.

18 Section 43. *Jurisdiction of cybercrime courts.* –

19 1. *Exclusive original jurisdiction* – The Cybercrime Court shall have exclusive original
20 jurisdiction over violations of this Act and over cases involving the Internet and information and
21 communications technology.

22 2. *Suit filed at the residence of the accused for criminal violations of the Magna Carta for*
23 *Philippine Internet Freedom.* – Except in cases that are extraterritorial, foreign, international, and
24 transnational in nature, all suits related to criminal violations of this Act shall be filed at the
25 cybercrime court having jurisdiction over the residence of the accused.

26 3. *Suit filed at the cybercrime court agreed upon by the parties for civil violations of the*
27 *Magna Carta for Philippine Internet Freedom.* – Except in cases that are extraterritorial, foreign,
28 international, and transnational in nature, all suits related to civil violations of this Act shall be

1 filed at the cybercrime court agreed upon by the parties. Should the parties be unable to reach an
2 agreement, the Court of Appeals shall determine the cybercrime court that shall have jurisdiction
3 over the case.

4 *Section 44. Extraterritorial application of the Magna Carta for Philippine Internet*
5 *Freedom. –*

6 1. *Extra-Territorial Application.* – Subject to the provision of an existing treaty of which
7 the Philippines is a State Party, and to any contrary provision of any law of preferential
8 application, the provisions of this Act shall apply:

9 (a) to individual persons who, although physically outside the territorial limits of
10 the Philippines, commit, conspire or plot to commit any of the crimes defined and
11 punished in this Act inside the territorial limits of the Philippines;

12 (b) to individual persons who, although physically outside the territorial limits of
13 the Philippines, commit any of the said crimes on board a Philippine ship or aircraft;

14 (c) to individual persons who commit any of said crimes within any embassy,
15 consulate, or diplomatic premises belonging to or occupied by the Philippine government
16 in an official capacity;

17 (d) to individual persons who, although physically outside the territorial limits of
18 the Philippines, commit said crimes against Philippine citizens or persons of Philippine
19 descent, where their citizenship or ethnicity was a factor in the commission of the crime;
20 and,

21 (e) to individual persons who, although physically outside the territorial limits of
22 the Philippines, commit said crimes directly against the Philippine government or critical
23 information and communications technology infrastructure in the Philippines.

1 **Part 4. Cyberdefense and National Cybersecurity.**

2 **Chapter X. National Cybersecurity and Cyberdefense.**

3 *Section 45. Cyberwarfare and National Defense. –*

4 1. It shall be unlawful for any person, or military or civilian agency, or instrumentality of
5 the State to initiate a cyberattack against any foreign nation, except in the event of a declaration
6 of a state of war with the foreign nation.

7 2. Subject to the Geneva Convention, the Hague Convention, the United Nations
8 Convention on Certain Conventional Weapons, other international treaties and conventions
9 governing the conduct of warfare, Philippine law, and the national interest, an authorized person
10 or military agency may engage in cyberattack against an enemy violent non-state actor, insurgent
11 group, or terrorist organization.

12 3. Subject to the Geneva Convention, the Hague Convention, the United Nations
13 Convention on Certain Conventional Weapons, other international treaties and conventions
14 governing the conduct of warfare, and Philippine law, an authorized person or military agency
15 may engage in cyberdefense in defense of the Filipino people, territory, economy, and vital
16 infrastructure in the event of a cyberattack by a foreign nation, enemy violent non-state actor,
17 insurgent group, or terrorist organization.

18 4. Any person who initiates an unauthorized and unlawful cyberattack against a foreign
19 nation shall be prosecuted under Commonwealth Act 408, as amended, or applicable military
20 law, without prejudice to criminal and civil prosecution.

21 *Section 46. National Cybersecurity and Protection of Government Information and*
22 *Communications Technology Infrastructure. –*

23 1. The Secretary of National Defense shall have the responsibility for national
24 cybersecurity and the protection of government information and communications technology
25 infrastructure.
26

27 2. The Secretary of Interior and Local Government shall assist the Secretary of National
28 Defense, and shall be jointly responsible for the cybersecurity of local government units and the
29 protection of local government information and communications technology infrastructure.

1 3. The Armed Forces of the Philippines shall be tasked with ensuring the physical and
2 network security of government and military information and communications infrastructure. In
3 cooperation with private and public owners, operators, and maintainers, the Philippine National
4 Police shall be tasked with ensuring the physical and network security of critical information and
5 communications infrastructure.

6 *Section 47. Amendments to the AFP Modernization Act. –*

7 1. Section 5 of the R.A. No. 7898 aka the “AFP Modernization Act” shall be amended to
8 include:

9 *Section 5. Development of AFP Capabilities. –* The AFP modernization
10 program shall be geared towards the development of the following defense
11 capabilities:

12 (d) Development of cyberdefense capability. – [The modernization of the
13 AFP further requires the development of the general headquarters capabilities for
14 command, control, communications, and information systems network.] **THE
15 PHILIPPINE AIR FORCE (PAF), BEING THE COUNTRY'S FIRST LINE
16 OF EXTERNAL DEFENSE, SHALL DEVELOP ITS CYBERDEFENSE
17 CAPABILITY. THE CYBERDEFENSE CAPABILITY SHALL ENABLE
18 THE AFP TO:**

19 **(1) DETECT, IDENTIFY, INTERCEPT AND ENGAGE, IF
20 NECESSARY, ANY ATTEMPTED OR ACTUAL PENETRATION
21 OR CYBERATTACK OF PHILIPPINE GOVERNMENT
22 INFORMATION AND COMMUNICATIONS TECHNOLOGY
23 INFRASTRUCTURE, AS WELL AS CRITICAL INFORMATION
24 AND COMMUNICATIONS TECHNOLOGY INFRASTRUCTURE
25 WITHIN PHILIPPINE JURISDICTION;**

26 **(2) PROVIDE CYBERDEFENSE SUPPORT TO
27 PHILIPPINE ARMED FORCES AND POLICE FORCES, AND;**

1 (3) PROVIDE, AND IF PRACTICABLE, INVENT OR
2 INNOVATE, THROUGH FILIPINO SKILLS AND TECHNOLOGY,
3 ITS OWN REQUIREMENTS FOR NATIONAL CYBERDEFENSE.

4 (E) DEVELOPMENT OF CYBERINTELLIGENCE CAPABILITY.
5 — THE INTELLIGENCE SERVICE OF THE ARMED FORCES OF THE
6 PHILIPPINES (ISAFP) OR ITS SUCCESSOR SERVICE, SHALL
7 DEVELOP ITS CYBERINTELLIGENCE CAPABILITY. THE
8 CYBERINTELLIGENCE CAPABILITY SHALL ENABLE THE AFP TO:

9 (1) DETECT ANY THREAT AGAINST PHILIPPINE
10 GOVERNMENT INFORMATION AND COMMUNICATIONS
11 TECHNOLOGY INFRASTRUCTURE, AS WELL AS CRITICAL
12 INFORMATION AND COMMUNICATIONS TECHNOLOGY
13 INFRASTRUCTURE WITHIN PHILIPPINE JURISDICTION, AND
14 IDENTIFY THE SOURCE OF THE THREAT, WHETHER
15 HOSTILE NATION-STATES, NON-STATE ACTORS,
16 CYBERTERRORISTS, OR CRIMINALS;

17 (2) PROVIDE CYBERINTELLIGENCE SUPPORT TO
18 PHILIPPINE ARMED FORCES AND POLICE FORCES, AND;

19 (3) PROVIDE, AND IF PRACTICABLE, INVENT OR
20 INNOVATE, THROUGH FILIPINO SKILLS AND TECHNOLOGY,
21 ITS OWN REQUIREMENTS FOR NATIONAL
22 CYBERINTELLIGENCE.

23 (F) DEVELOPMENT OF GOVERNMENT AND MILITARY
24 INFORMATION AND COMMUNICATIONS TECHNOLOGY
25 INFRASTRUCTURE HARDENED AGAINST CYBERATTACK. — THE
26 COMMUNICATIONS, ELECTRONICS AND INFORMATION SYSTEM
27 SERVICE, ARMED FORCES OF THE PHILIPPINES (CEISSAFP) OR
28 ITS SUCCESSOR SERVICE, SHALL CONTINUALLY ENSURE THAT
29 GOVERNMENT AND MILITARY INFORMATION AND

1 **COMMUNICATIONS TECHNOLOGY INFRASTRUCTURE ARE**
2 **HARDENED AGAINST CYBERATTACK.**

3 **Chapter XI. Counter-Cyberterrorism.**

4 *Section 48. Counter-Cyberterrorism. –*

5 1. The Philippine National Police, supported by applicable military, law enforcement, and
6 government services, offices, and agencies, shall be the lead law enforcement agency responsible
7 for plans, policies, programs, measures, and mechanisms to detect, identify, and prevent
8 cyberterrorist attacks on Philippine government information and communications technology
9 infrastructure, as well as publicly- and privately-owned information and communications
10 technology infrastructure within Philippine jurisdiction, and the detection, identification, pursuit,
11 apprehension, and the gathering of evidence leading to the conviction of persons committing
12 cyberterrorism.

13 2. The National Bureau of Investigation, supported by applicable military, law
14 enforcement, and government services, offices, and agencies, shall be the lead law enforcement
15 agency responsible for plans, policies, programs, measures, and mechanisms to detect, identify,
16 and prevent transnational cyberterrorist attacks on Philippine government information and
17 communications technology infrastructure, as well as publicly- and privately-owned information
18 and communications technology infrastructure within Philippine jurisdiction

19 3. Subject to the provisions of an existing treaty to which the Philippines is a signatory
20 and to any contrary provision of any law of preferential application, and subject to the
21 concurrence of the Secretary of Justice and the Secretary of Foreign Affairs, the Director of the
22 National Bureau of Investigation may cooperate with or request the cooperation of foreign or
23 international law enforcement agencies in the detection, identification, pursuit, apprehension, and
24 the gathering of evidence leading to the conviction of persons who, although physically outside
25 the territorial limits of the Philippines, have committed or are attempting to commit acts of
26 cyberterrorism within Philippine jurisdiction.

1 **Part 5. Final Provisions**

2 **Chapter XII. Implementing Rules and Regulations.**

3 *Section 49. General Implementing Rules and Regulations for the Implementation of the*
4 *Magna Carta for Philippine Internet Freedom. –*

5 1. The Secretary of Information and Communication Technology, the Commissioner of
6 the National Telecommunications Commission, the Commissioner of the National Data Privacy
7 Commission, or the Chief of the Telecommunications Office, or their duly authorized and
8 appointed delegates, an appointee from the academe, and an appointee from the business sector
9 shall be jointly responsible for the creation of general implementing rules and regulations (IRR)
10 of this Act. The Solicitor-General shall participate to ensure that the IRR is not in conflict with
11 this Act, with other laws, with other IRRs of this Act, and with generally accepted principles of
12 international human, civil, and political rights.

13 2. The General Implementing Rules and Regulations for the Implementation of the
14 Magna Carta for Philippine Internet Freedom shall be made public after its approval.

15 3. The President shall implement the General Implementing Rules and Regulations for
16 the Implementation of the Magna Carta for Philippine Internet Freedom through the applicable
17 agencies and instrumentalities of the Executive.

18 *Section 50. Implementing Rules and Regulations for Information and Communications*
19 *Technology Infrastructure Development. –*

20 1. The Secretary of Information and Communication Technology, the Secretary of
21 Finance, the Director-General of the National Economic and Development Authority, the
22 Chairman of the Board of Investments, or their duly authorized and appointed delegates, an
23 appointee from the academe, and an appointee from the business sector shall be jointly
24 responsible for the creation of implementing rules and regulations (IRR) of this Act towards the
25 development of information and communications technology infrastructure. The Solicitor-
26 General shall participate to ensure that the IRR is not in conflict with this Act, with other laws,
27 with other IRRs of this Act, and with generally accepted principles of international human, civil,
28 and political rights.

1 2. The IRR for ICT Infrastructure Development shall be made public after its approval.

2 3. The President shall implement the IRR for Information and Communications
3 Technology Infrastructure Development through the applicable agencies and instrumentalities of
4 the Executive.

5 *Section 51. Implementing Rules and Regulations for Cybercrime Law Enforcement. –*

6 1. The Secretary of Information and Communication Technology, the Secretary of
7 Justice, the Secretary of Interior and Local Government, the Secretary of Social Welfare and
8 Development, , the Secretary of Foreign Affairs, the Director-General of the National Bureau of
9 Investigation, the the Director-General of the Philippine National Police, or their duly authorized
10 and appointed delegates, an appointee from the academe, an appointee from civil society, and an
11 appointee from the business sector shall be jointly responsible for the creation of implementing
12 rules and regulations (IRR) of this Act towards cybercrime and law enforcement. The Solicitor-
13 General and the Chairman of the Commission on Human Rights shall participate to ensure that
14 the IRR is not in conflict with this Act, with other laws, with other IRRs of this Act, and with
15 generally accepted principles of international human, civil, and political rights.

16 2. The IRR for Cybercrime and Law Enforcement shall be made public after its approval.

17 3. The President shall implement the IRR for Cybercrime and Law Enforcement through
18 the applicable agencies and instrumentalities of the Executive.

19 *Section 52. Implementing Rules and Regulations for Information and Communications*
20 *Technology Education, Training, and Human Resources. –*

21 1. The Secretary of Information and Communication Technology, the Secretary of
22 Education, the Secretary of Science and Technology, the Commissioner of Higher Education, the
23 Director-General of the Technical Education and Skills Development Authority, the Head of the
24 National Telecommunications Training Institute, or their duly authorized and appointed
25 delegates, and an appointee from the academe, shall be jointly responsible for the creation of
26 implementing rules and regulations (IRR) of this Act towards information and communications
27 technology education, training and human resources. The Solicitor-General and the Secretary of
28 Labor and Employment shall participate to ensure that the IRR is not in conflict with this Act,

1 with other laws, with other IRRs of this Act, and with generally accepted principles of
2 international human, civil, and political rights.

3 2. The IRR for ICT Education, Training and Human Resources shall be made public after
4 its approval.

5 3. The President shall implement the IRR for ICT Education, Training and Human
6 Resources through the applicable agencies and instrumentalities of the Executive.

7 *Section 53 Implementing Rules and Regulations for Information and Communications*
8 *Technology Research and Development.* –

9 1. The Secretary of Information and Communication Technology, the the Secretary of
10 Science and Technology, the Director-General of the National Economic and Development
11 Authority, or their duly authorized and appointed delegates, an appointee from the academe, and
12 an appointee from the business sector, shall be jointly responsible for the creation of
13 implementing rules and regulations (IRR) of this Act towards information and communications
14 technology research and development. The Solicitor-General shall participate to ensure that the
15 IRR is not in conflict with this Act, with other laws, with other IRRs of this Act, and with
16 generally accepted principles of international human, civil, and political rights.

17 2. The IRR for ICT Research and Development shall be made public after its approval.

18 3. The President shall implement the IRR for ICT Research and Development through the
19 applicable agencies and instrumentalities of the Executive.

20 *Section 54. Implementing Rules and Regulations for National Cyberdefense,*
21 *Cyberintelligence, and Counter-Cyberterrorism.* –

22 1. The Secretary of National Defense, the Secretary of Interior and Local Government, or
23 their duly authorized and appointed delegates, the Chief of Staff of the Armed Forces of the
24 Philippines (AFP), the commanding general of the unit of the Philippine Air Force tasked with
25 national cyberdefense, the commanding officer of the Intelligence Service, Armed Forces of the
26 Philippines (ISAFP), the commanding officer of the Communication Electronics and Information
27 Systems Service, Armed Forces of the Philippines (CEISSAFP), and the Director-General of the
28 Philippine National Police shall be jointly responsible for the creation of implementing rules and

1 regulations (IRR) of this Act towards ensuring national cyberdefense, cyberintelligence, and
2 counter-cyberterrorism. The Secretary of Information and Communication Technology shall
3 provide technical advice. The Solicitor-General and the Chairman of the Commission on Human
4 Rights shall participate to ensure that the IRR is not in conflict with this Act, with other laws,
5 with other IRRs of this Act, and with generally accepted principles of international human, civil,
6 and political rights.

7 2. An executive summary of the IRR for National Cyberdefense, Cyberintelligence, and
8 Counter-Cyberterrorism shall be allowed to be made public after the approval of the IRR. Any
9 review of any portion of the IRR for National Cyberdefense, Cyberintelligence, and Counter-
10 Cyberterrorism shall be done in special executive sessions for this purpose.

11 3. Subject to the approval of the President, and subject to the advice and consent of the
12 Joint Select Committee on Military and Intelligence Affairs of the House of Representatives and
13 the Senate, the The Secretary of National Defense, the Secretary of Interior and Local
14 Government, or their duly authorized and appointed delegates, the Chief of Staff of the Armed
15 Forces of the Philippines (AFP), the commanding general of the unit of the Philippine Air Force
16 tasked with national cyberdefense, the commanding officer of the Intelligence Service, Armed
17 Forces of the Philippines (ISAFP), the commanding officer of the Communication Electronics
18 and Information Systems Service, Armed Forces of the Philippines (CEISSAFP), and the
19 Director-General of the Philippine National Police shall prepare a National Cyberdefense and
20 Counter-Cyberterrorism Plan every three years.

21 4. The President shall have the power to implement the National Cyberdefense and
22 Counter-Cyberterrorism Plan.

23 5. The contents of the current and past National Cyberdefense and Counter-
24 Cyberterrorism Plans shall be considered state secrets, and disclosure shall be punishable to the
25 fullest extent possible by relevant laws.

1 *Section 55. Implementing Rules and Regulations for Government Information and*
2 *Communications Infrastructure and National Cybersecurity. –*

3 1. The Secretary of Information and Telecommunications, the Secretary of National
4 Defense, and the Secretary of Interior and Local Government, or their duly authorized and
5 appointed delegates, the commanding general of the unit of the Philippine Air Force tasked with
6 national cyberdefense, and the commanding officer of the Communication Electronics and
7 Information Systems Service, Armed Forces of the Philippines (CEISSAFP) shall be jointly
8 responsible for the creation of implementing rules and regulations (IRR) of this Act towards
9 securing government information and communications infrastructure. The Secretary of
10 Information and Communication Technology shall provide technical advice. The Solicitor-
11 General and the Chairman of the Commission on Human Rights shall participate to ensure that
12 the IRR is not in conflict with this Act, with other laws, with other IRRs of this Act, and with
13 generally accepted principles of international human, civil, and political rights.

14 2. Subject to the approval of the President, and subject to the advice and consent of the
15 Joint Select Committee on Military and Intelligence Affairs of the House of Representatives and
16 the Senate, the Secretary of Information and Telecommunications, the Secretary of National
17 Defense, and the Secretary of Interior and Local Government, or their duly appointed delegates,
18 the commanding general of the unit of the Philippine Air Force tasked with national
19 cyberdefense, and the commanding officer of the Communication Electronics and Information
20 Systems Service, Armed Forces of the Philippines (CEISSAFP) shall prepare a National
21 Cybersecurity Plan every three years.

22 3. The plans, policies, programs, measures, and mechanisms of the National
23 Cybersecurity Plan shall be used to secure government information and communications
24 infrastructure and to secure critical data, network, Internet, or telecommunications infrastructure.

25 4. The IRR for National Cybersecurity shall be made public after its approval.

26 5. The President shall implement the National Cybersecurity Plan through the applicable
27 agencies and instrumentalities of the Executive.

28 6. The contents of the current National Cybersecurity Plan shall be considered state
29 secrets, and disclosure shall be punishable to the fullest extent possible by relevant laws.

1 **Chapter XIII. Periodic Review Clause.**

2 *Section 56. Periodic Review of the Implementing Rules and Regulations of the Magna*
3 *Carta for Philippine Internet Freedom. –*

4 1. Mandatory and periodic reviews of the implementing rules and regulations of the
5 Magna Carta for Philippine Internet Freedom shall be done by the offices designated by this Act
6 to create implementing rules and regulations. Such reviews shall be performed no less than every
7 three years and no more than every five years, to keep pace with technological advancements and
8 other changes.

9 2. Periodic reviews of the implementing rules and regulations and the recommendation of
10 the improvement of the Magna Carta for Philippine Internet Freedom shall be done by the offices
11 designated by this Act to create implementing rules and regulations, to keep pace with
12 technological advancements and other changes.

13 **Chapter XIV. Transitory Provisions.**

14 *Section 57. Appointment of the Secretary of Information and Communications*
15 *Technology. –* Subject to confirmation by the Commission on Appointments, the President shall
16 appoint the Secretary of Information and Communications Technology within 30 days of the
17 effectivity of this Act.

18 *Section 58. Release of Initial Appropriations. –* Subject to government budgetary and
19 audit procedures, the Department of Budget and Management shall release appropriations to the
20 Secretary of Information and Communications Technology for purposes of implementing this
21 Act within 30 days of his appointment.

22 *Section 59. Preparation of Implementing Rules and Regulations. –* Within 90 days of the
23 release of initial appropriations, implementing rules and regulations shall have been prepared and
24 approved. The National Cyberdefense and Counter-Cyberterrorism Plan and the National
25 Cybersecurity Plan shall be prepared, approved, and implemented within 90 days of the approval
26 of the implementing rules and regulations.

1 *Section 60. Compliance of Government ICT Infrastructure and Critical Networks, Data,*
2 *and Internet Infrastructure. –*

3 1. Within 90 days of the approval of the National Cybersecurity Plan, government
4 agencies and instrumentalities shall have secured their private network and data infrastructure as
5 prescribed by the Plan. Penalties as prescribed by this Act shall be imposed for noncompliance.

6 2. Within 180 days of the approval of the National Cybersecurity Plan, government
7 agencies and instrumentalities shall have secured their public network, data, and Internet
8 infrastructure as prescribed by the Plan. Penalties as prescribed by this Act shall be imposed for
9 noncompliance.

10 3. Within 180 days of the approval of the National Cybersecurity Plan, all Internet service
11 providers, Internet exchanges, Internet data centers, Internet gateway facilities,
12 telecommunications entities, and persons providing Internet connection, network, or data
13 transmission services shall have met the minimum standards of privacy and security for their
14 private and public network, data, and Internet infrastructure as prescribed by the Plan and
15 appropriate official instructions. Penalties as prescribed by this Act shall be imposed for
16 noncompliance.

17 4. Within 60 days of the approval of the implementing rules and regulations, all Internet
18 service providers, Internet exchanges, Internet data centers, Internet gateway facilities,
19 telecommunications entities, and persons providing Internet connection, network, or data
20 transmission services shall have met the minimum standards of interconnectivity and
21 interoperability of their information and communications technology infrastructure as prescribed
22 by the implementing rules and regulations and appropriate official instructions. Administrative
23 penalties shall be prescribed for noncompliance.

24 5. Within 90 days of the approval of the implementing rules and regulations, all Internet
25 service providers, Internet exchanges, Internet data centers, Internet gateway facilities,
26 telecommunications entities, and persons providing Internet connection, network, or data
27 transmission services shall have met the minimum standards of service quality as prescribed by
28 the implementing rules and regulations and appropriate official instructions. Administrative
29 penalties shall be prescribed for noncompliance.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

Chapter XV. Public Information Campaign.

Section 61. Public Information Campaign for the Magna Carta for Philippine Internet Freedom and its Implementing Rules and Regulations. –

1. The Office of the President, the Presidential Communications Development and Strategic Planning Office or its successor agency, the Philippine Information Agency or its successor agency, and the Department of Interior and Local Government through the information offices of local government units, shall be jointly responsible for information campaigns to ensure nationwide awareness of the Magna Carta for Philippine Internet Freedom and its implementing rules and regulations.

2. The Department of Education and the Department of Social Welfare and Development may provide age-appropriate information campaigns in schools to ensure nationwide awareness of the Magna Carta for Philippine Internet Freedom, its implementing rules and regulations, and the safe use of the Internet and information and communications technology for children of school age and for out-of-school youths.

Chapter XVI. Appropriations.

Section 62. Initial funding requirements. –

1. DICT – An initial appropriation of fifteen million pesos (PHP 15,000,000) shall be drawn from the national government for purposes of establishment and operation of the DICT, exclusive of the existing appropriations of its subordinate agencies.

2. DOJ – The initial funding requirements for the implementation of this Act of the DOJ shall be charged against the current appropriations of the DOJ.

3. NBI – The initial funding requirements for the implementation of this Act of the NBI shall be charged against the current appropriations of the NBI.

4. PNP – The initial funding requirements for the implementation of this Act of the PNP shall be charged against the current appropriations of the PNP.

5. IRR – An initial appropriation of five million pesos (PHP 5,000,000), to be disbursed by the Secretary of Information and Communications Technology, shall be drawn from the

1 national government for purposes of the preparation of the Implementing Rules and Regulations
2 of this Act.

3 6. PIA – An initial appropriation of five million pesos (PHP 5,000,000) shall be drawn
4 from the national government for purposes of the information dissemination campaign on this
5 Act by the PIA.

6 7. Other agencies – The initial funding requirements for the implementation of this Act
7 by other agencies shall be charged against the current appropriations of the respective agencies.

8
9 *Section 63. Succeeding appropriations.* – Such sums as may be necessary for the
10 implementation of this Act shall be included in the agencies' yearly budgets under the General
11 Appropriations Act.

12 **Chapter XVII. Separability Clause.**

13 *Section 64. Separability clause.* – If any provision or part hereof is held invalid or
14 unconstitutional, the remainder of the law or the provisions not otherwise affected shall remain
15 valid and subsisting.

16 **Chapter XVIII. Repealing Clause.**

17 *Section 65. Repealing clause* – Any law, presidential decree or issuance, executive order,
18 letter of instruction, administrative order, rule, or regulation contrary to, or inconsistent with, the
19 provisions of this Act is hereby repealed, modified, or amended accordingly.

20 **Chapter XIX. Effectivity Clause**

21 *Section 66. Effectivity clause.* – This Act shall take effect fifteen (15) days after its online
22 publication in the Official Gazette. Within seven (7) days after its online publication, this Act
23 shall be published on (2) newspapers of general circulation.

Approved,